ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Ανάπτυξη Τυποποιημένου και Ολοκληρωμένου Ταξινομικού Συστήματος για την Κοινοποίηση Πληροφοριών Κυβερνοαπειλών (Cyber Threat Intelligence - CTI)»

Του φοιτητή
ΜΠΕΚΑ ΠΑΣΧΑΛΗ
Αρ. Μητρώου: 16/2023

Επιβλέπων
ΧΑΡΑΛΑΜΠΟΣ ΜΠΡΑΤΣΑΣ
Βαθμίδα ……

Ημερομηνία ……

Κεφάλαιο 1

Τίτλος Δ.Ε. «Ανάπτυξη Τυποποιημένου και Ολοκληρωμένου Ταξινομικού Συστήματος για την Κοινοποίηση Πληροφοριών Κυβερνοαπειλών (Cyber Threat Intelligence - CTI)».
Κωδικός Δ.Ε. 24263
Ονοματεπώνυμο φοιτητή Πασχάλης Μπέκας
Ονοματεπώνυμο εισηγητή Χαράλαμπος Μπράτσας
Ημερομηνία ανάληψης Δ.Ε. 21/10/2024
Ημερομηνία περάτωσης Δ.Ε. 26/05/2025

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

«Αφιέρωση»

Πρόλογος

Η επιλογή του θέματος αυτής της διπλωματικής εργασίας δεν ήταν τυχαία. Η κυβερνοασφάλεια αποτελεί έναν διαρκώς εξελισσόμενο τομέα, με ολοένα και μεγαλύτερες προκλήσεις και πάντα με γοήτευε αυτός ο χώρος. Το γεγονός ότι οι πληροφορίες για τις κυβερνοαπειλές είναι συχνά αποσπασματικές και ελλιπώς δομημένες, με έκανε να αναζητήσω την διαδικασία που θα μπορούσε να προσφέρει η καλύτερη οργάνωση αυτής της πληροφορίας.
Η επιλογή του SKOS ως μοντέλου για την οντολογία της παρουσίασης, προέκυψε από την ανάγκη για ένα ευέλικτο και πρακτικό εργαλείο που θα μπορούσε να συνδέσει τα δεδομένα και να ενισχύσει την ανάλυση και την ανταλλαγή των πληροφοριών στον ευρύ τομέα της κυβερνοασφάλειας και στο Cyber Threat Intelligence (CTI).
Η ενασχόλησή μου με αυτό το αντικείμενο μου έδωσε πολύτιμες γνώσεις τόσο σε τεχνικό όσο και σε θεωρητικό επίπεδο. Μέσα από τη μελέτη και την ανάπτυξη της οντολογίας, κατανόησα καλύτερα τις τεχνολογίες Σημασιολογικού Ιστού, στη διαχείριση δομημένης πληροφορίας. Επιπλέον, η διαδικασία αυτή με βοήθησε να αναπτύξω αναλυτική σκέψη και δεξιότητες μοντελοποίησης, που θα είναι χρήσιμες στην επαγγελματική μου πορεία.

Περίληψη

Στη σημερινή εποχή, οι κυβερνοαπειλές εξελίσσονται και αυξάνονται με ραγδαίους ρυθμούς, γι' αυτό και υπάρχει η ανάγκη για μία καλά οργανωμένη και αποδοτική διαχείριση της πληροφορίας που έχει να κάνει με την κυβερνοασφάλεια. Το Cyber Threat Intelligence (CTI) ως ένα υπό τομέας του cybersecurity, μπορεί να παρέχει τη γνώση που απαιτείται για την αναγνώριση και αντιμετώπιση κακόβουλων ενεργειών, αλλά λόγο έλλειψης σαφούς δομής και διαλειτουργικότητας στα δεδομένα πληροφορίας του CTI, καθιστά δύσκολο την ανάλυση και την ανταλλαγή πληροφοριών.

Η παρούσα διπλωματική εργασία επικεντρώνεται κυρίως στη δημιουργία μιας οντολογίας-λεξικού βασισμένης στο μοντέλο SKOS (Simple Knowledge Organization System), η οποία θα προβάλει με ιεραρχία και οργάνωση έννοιες που σχετίζονται με τις κυβερνοαπειλές. Με τη χρήση του SKOS, θα αναπτυχθεί μία ιεραρχία εννοιών όπως Threat Actors, Tactics, Techniques & Procedures (TTPs), Malware και Indicators of Compromise (IoCs), Vulnerabilities και είδη αυτών, παρέχοντας μια δομημένη και επεκτάσιμη προσέγγιση στην κατηγοριοποίηση των μορφών απειλών που μπορεί να υπάρχουν στον κυβερνοχώρο.

Στο πλαίσιο αυτής της μελέτης, θα εξεταστούν υπάρχουσες ταξινομίες-θησαυροί και οντολογίες-λεξικά στον χώρο της κυβερνοασφάλειας, ενώ θα διερευνηθεί και η μελλοντική διασύνδεση της προτεινόμενης οντολογίας με δημοφιλή πρότυπα, όπως το MITRE ATT&CK και το STIX. Επιπλέον, θα παρουσιαστεί η διαδικασία που ακολουθήθηκε για την ανάπτυξη της ανωτέρω οντολογίας, καθώς και οι τεχνολογίες που χρησιμοποιήθηκαν, όπως το Protege, RDF.

Μέσα από αυτή την προσέγγιση, η εργασία αποδεικνύει πως η χρήση τεχνολογιών σημασιολογικού ιστού στο CTI μπορεί να βελτιώσει τη διαχείριση της πληροφορίας στην ασφάλεια, να ενισχύσει την κατανόηση και την αναγνώριση των απειλών που υπάρχουν και να συμβάλει στη αποτελεσματικότητα των συστημάτων του cybersecurity.

«Development of a Standardized and Integrated Taxonomy System for the Communication of Cyber Threat Intelligence (CTI)»

«Paschalis Bekas»

Abstract

In today's era, cyber threats are evolving and increasing rapidly, which is why there is a need for a well-organized and efficient management of information related to cybersecurity. Cyber Threat Intelligence (CTI) as a sub-field of cybersecurity, can provide the knowledge required to identify and respond to malicious actions, but due to the lack of a clear structure and interoperability in CTI information data, it makes it difficult to analyze and exchange information.

This research focuses mainly on the creation of an ontology-dictionary based on the SKOS (Simple Knowledge Organization System) model, which will present concepts related to cyber threats in a hierarchical and organized manner. Using SKOS, a hierarchy of concepts such as Threat Actors, Tactics, Techniques & Procedures (TTPs), Malware and Indicators of Compromise (IoCs), Vulnerabilities and their types will be developed, providing a structured and extensible approach to the categorization of the types of threats that may exist in cyberspace.

In the context of this study, existing taxonomies-thesauri and ontologies-dictionaries in the field of cybersecurity will be examined, while the future interconnection of the proposed ontology with popular standards, such as MITRE ATT&CK and STIX, will be explored. In addition, the process followed for the development of the above ontology will be presented, as well as the technologies used, such as Protege, RDF.

Through this approach, the work demonstrates how the use of semantic web technologies in CTI can improve security information management, enhance the understanding and identification of existing threats, and contribute to the effectiveness of cybersecurity systems.

Ευχαριστίες

Η ολοκλήρωση αυτής της διπλωματικής εργασίας δεν θα ήταν δυνατή χωρίς τη στήριξη και την καθοδήγηση σημαντικών ανθρώπων στη ζωή μου, στους οποίους οφείλω ένα μεγάλο «ευχαριστώ».

Πρώτα απ' όλα, θέλω να ευχαριστήσω την οικογένειά μου, που ήταν πάντα δίπλα μου, με υπομονή, ενθάρρυνση και αγάπη. Σε κάθε δύσκολη στιγμή, η στήριξή τους μου έδινε τη δύναμη να συνεχίσω.

Ένα ιδιαίτερο ευχαριστώ στη σύζυγό μου, που στάθηκε βράχος σε αυτή τη διαδρομή. Με την κατανόηση, την αστείρευτη υπομονή και την αδιάκοπη υποστήριξή της, έκανε τις απαιτητικές στιγμές πιο εύκολες και με βοήθησε να παραμείνω συγκεντρωμένος στον στόχο μου. Χωρίς εκείνη, αυτό το ταξίδι θα ήταν πολύ πιο δύσκολο.

Τέλος, θέλω να εκφράσω την ειλικρινή μου ευγνωμοσύνη στον επιβλέποντα καθηγητή μου, που με τις πολύτιμες συμβουλές, την καθοδήγηση και την αφοσίωσή του με βοήθησε να αναπτύξω αυτή την εργασία. Η υποστήριξή του και η εμπιστοσύνη του στις δυνατότητές μου αποτέλεσαν καταλυτικούς παράγοντες για την ολοκλήρωση της.

Σε όλους εσάς, ένα μεγάλο ευχαριστώ από καρδιάς. Αυτή η εργασία είναι και δικό σας επίτευγμα.

Περιεχόμενα

Πρόλογος iv
Περίληψη v
Abstract vi
Ευχαριστίες vii
Περιεχόμενα viii
Κατάλογος Εικόνων x
Κατάλογος Πινάκων xi
Συντομογραφίες xii
Κεφάλαιο 1ο: Εισαγωγή 13
1.1 Σκοπός και στόχοι της εργασίας 13
1.2 Δομή της εργασίας 14
Κεφάλαιο 2ο: Θεωρητικό υπόβαθρο 15
2.1 Οντολογίες, Ταξινομίες και Θησαυροί 15
2.1.1 Οντολογία 15
2.1.2 Ταξινομία 15
2.1.3 Θησαυροί 16
2.2 Χρήση στην αναπαράσταση γνώσης 16
2.3 Cyber Threat Intelligence (CTI) 18
2.3.1 Ορισμός και σημασία 18
2.3.2 Βασικές έννοιες και πρότυπα (π.χ. STIX, TAXII, MITRE ATT&CK) 19
STIX (Structured Threat Information eXpression) 19
TAXII (Trusted Automated Exchange of Indicator Information) 20
MITRE ATT&CK 21
2.4 Μοντέλα στο Cyber Threat Intelligence 22
2.4.1 The Diamond Model of Intrusion Analysis 22
2.4.3 The Detection Maturity Level (DML) 25
2.4.4 The Cyber Threat Intelligence (CTI) Model 26
Κεφάλαιο 3ο: SKOS (Simple Knowledge Organization System) 30
3.1 Τι είναι το SKOS; 30
3.2 Κύρια χαρακτηριστικά του SKOS 30
3.2.1 skos:Consept 30
3.2.2 skos:ConseptSheme 31
3.2.3 skos:Collection 31
3.2.4 skos:OrderedCollection 31

3.2.5 Ετικέτες 32
3.2.6 Σημασιολογικές Σχέσεις 33
3.2.7 Χαρτογράφηση Σχέσεων 33
3.2.8 Ιδιότητες Τεκμηρίωσης 34
3.2.9 Ιδιότητες Συλλογών 35
3.2.10 Χρήση του SKOS στην Αναπαράσταση Εννοιών 36
3.3 Σύγκριση SKOS με άλλα μοντέλα 37
3.3.1 Σύγκριση SKOS με OWL 37
3.3.2 Σύγκριση SKOS με STIX 38
3.3.3 Σύγκριση SKOS με Θησαυρούς 38
3.4 Πρακτική Χρήση του SKOS στο CTI 40
Κεφάλαιο 4ο: Μεθοδολογία 42
4.1 Ορισμός στόχων και απαιτήσεων 42
4.2 Συλλογή και ανάπτυξη δεδομένων 42
4.3 Ανάπτυξη της οντολογίας στο Protégé 47
4.3.1 Εγκατάσταση και δημιουργία νέου Project 47
4.3.2 Δημιουργία Κύριου Σχήματος 48
4.3.3 Ορισμός Κύριων Εννοιών (Concepts) 51
4.4 Ανάλυση Οντολογίας 65
Κεφάλαιο 5ο: Συμπεράσματα και προτάσεις βελτίωσης 70
ΠΑΡΑΡΤΗΜΑ Α : Script Python για την εξαγωγή των CVEs 72
ΠΑΡΑΡΤΗΜΑ Β: Script Python για την εξαγωγή γραφημάτων 73
ΠΑΡΑΡΤΗΜΑ Γ: Οντολογία σε μορφή .ttl με τις κύριες έννοιες 75
ΒΙΒΛΙΟΓΡΑΦΙΑ 79

Κατάλογος Εικόνων

Εικόνα 1 - Kinds of ontologies, according to their level of dependence on a particular (https://www.loa.istc.cnr.it/old/Papers/FOIS98.pdf)..... 17
Εικόνα 2 - STIX Architecture [https://oasis-open.github.io/cti-documentation/stix/intro]. 20
Εικόνα 3 - TAXII sharing models..... 21
Εικόνα 4 - The Diamond Model of Intrusion Analysis (Sergio Caltagirone). 22
Εικόνα 5 - The Cyber Kill Chain (https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html)..... 24
Εικόνα 6 - The Detection Maturity Level Model (Bromander 2017). 25
Εικόνα 7 - Cyber Threat Intelligence Model (Bromander 2017). 27
Εικόνα 8 - Γράφημα RDF με λεξικό SKOS Core (Brickley 2005)..... 37
Εικόνα 9 - Πλεονεκτήματα του SKOS σε σχέση με άλλες ενναλακτικές δημιουργίας θησαυρών (Juan-Antonio Pastor-Sanchez 2009) 40
Εικόνα 10 - Imported Ontologies in Protégé..... 48
Εικόνα 11 - Εισαγωγή Cybersecurity Taxonomy της EU. 48
Εικόνα 12 - Concept Scheme Annotations..... 49
Εικόνα 13 - Top Concept Annotations..... 49
Εικόνα 14 - Ιεραρχία CYBERSECURITY GLOSSARY 50
Εικόνα 15 - Ιεραρχία μοντέλου σε Γράφο. 50
Εικόνα 16 - Κύριες έννοιες-τομείς οντολογίας..... 51
Εικόνα 17 - Atomic Indicators Concept..... 52
Εικόνα 18 - Courses of Actions 54
Εικόνα 19 - Identity..... 55
Εικόνα 20 - Indicators of Compromise (IoCs). 56
Εικόνα 21 – Motivation..... 56
Εικόνα 22 - TTPs 57
Εικόνα 23 - Tactics..... 58
Εικόνα 24 - Attack Techniques 58
Εικόνα 25 - Procedures 59
Εικόνα 26 – Target..... 60
Εικόνα 27 - Vulnerabilities 61
Εικόνα 28 - Μορφή αρχείου CVEs..... 61
Εικόνα 29 - Script μετατροπής σε μορφή Turtle..... 62
Εικόνα 30 - Μορφή Turtle των CVEs..... 62
Εικόνα 31 - Διάγραμμα ροής Βημάτων CVSS 64
Εικόνα 32 - Ontology Metrics..... 65
Εικόνα 33 - Ontology Entities Overview 66
Εικόνα 34 - Main Axiom Types..... 66
Εικόνα 35 - Object Property Axioms 67
Εικόνα 36 - Class Axioms..... 67
Εικόνα 37 - Data property Axioms 68
Εικόνα 38 - Individual Axioms..... 68
Εικόνα 39 - Annotations Axioms..... 69
Εικόνα 40 - Διασύνδεση SKOS CTI Ontology με Πρότυπα και Πλατφόρμες..... 71

Κατάλογος Πινάκων

Πίνακας 1 - Ανάλυση κύριων κλάσεων SKOS 32
Πίνακας 2 - Ανάλυση ιδιοτήτων SKOS 35
Πίνακας 3 - Σύγκριση SKOS με OWL 38
Πίνακας 4 - Σύγκριση SKOS με STIX 38
Πίνακας 5 - Σύγκριση SKOS με THESAURUS 39
Πίνακας 6 - CVSS 63

Συντομογραφίες

AI	Artificial Intelligence
ATT&CK	Adversarial Tactics Techniques, and Common Knowledge
CAPEC	Common Attack Pattern Enumeration and Classification
CoA	Courses of Action
CTI	Cyber Threat Intelligence
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DML	Detection Maturity Level
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
IoC	Indicators of Compromise
IoT	Internet of Things
NSM	Network Security Monitoring
NVD	National Vulnerability Database
OSINT	Open-Source Intelligence
OWL	Web Ontology Language
OWL	Web Ontology Language
RDF	Resource Description Framework
S-MAIDS	Semantic Model of Automated Intrusion Detection Systems
SIEM	Security Information Event Management
SMEs	Small and Medium sized Enterprises
SOC	Security Operations Center
SPARQL	SPARQL Protocol and RDF Query Language
STIX	Structured Threat Information eXpression
TIP	Threat Intelligence Platform
TTP	Tactics, Techniques and Procedures
UI	User Interfaces
URI	Uniform Resource Identifier
XSS	Cross-Site Scripting

Κεφάλαιο 1ο: Εισαγωγή

Η τεχνολογία συνεχώς αυξάνεται και μαζί της αυξάνονται και οι ανάγκες σε νέα προϊόντα ή υπηρεσίες και αυτό έχει ως εξέλιξη την εξάρτησή μας από την τεχνολογία. Ωστόσο αυξάνεται και η σημασία της κυβερνοασφάλειας καθώς τροφοδοτούμε το διαδίκτυο όλο και περισσότερο με δεδομένα προσωπικού χαρακτήρα, όσο περισσότερο είμαστε συνδεδεμένοι σε αυτό αυξάνονται κατά πολύ και οι πιθανότητες να γίνουμε θύματα μίας κυβερνοεπίθεσης ή κυβερνοεγκλήματος.
Στον σύγχρονο κυβερνοχώρο, η ασφάλεια αποτελεί κρίσιμο παράγοντα για οργανισμούς, εταιρίες, κυβερνήσεις και ιδιώτες. Η κυβερνοασφάλεια χαρακτηρίζεται στην πρόληψη και την ανίχνευση περιστατικών στον κυβερνοχώρο, την αντίδραση και την ανάκαμψη από αυτά. Τα περιστατικά αυτά κυμαίνονται από την τυχαία ή όχι κοινολόγηση πληροφοριών έως επιθέσεις τις περισσότερες κατά οργανισμών καθώς και υποδομών ζωτικής σημασίας, την κλοπή ευαίσθητων δεδομένων, ακόμη και έως ενέργειες σε δημοκρατικές διαδικασίες. Όλα αυτά μπορούν να έχουν ποικίλες ζημίες και επιδράσεις σε πρόσωπα, οργανισμούς, κοινότητες, κράτη.
Οι Οργανισμοί εξαρτώνται όλο και περισσότερο από την τεχνολογία στον τομέα της πληροφορικής και επικοινωνιών για να επιτύχουν την λειτουργία και αποστολή τους. Οι εν λόγω τεχνολογίες έχουν φυσικά θετικά αλλά και αρνητικά στοιχεία και υπόκεινται σε απειλές, οι οποίες στοχεύουν σε γνωστές και άγνωστες ευπάθειες των πληροφοριακών συστημάτων και συχνά έχουν σοβαρές επιπτώσεις στην επιχειρησιακή λειτουργία, στα πρόσωπα που τις περιβάλουν, στις υποδομές, ακόμη και στην εθνική ασφάλεια της κάθε χώρας, λόγω της παραβίασης της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας της πληροφορίας που τα πληροφοριακά συστήματα διαχειρίζονται, αποθηκεύουν ή μεταδίδουν. Οι απειλές για τις τεχνολογίες πληροφορικής περιλαμβάνουν τις κυβερνοεπιθέσεις, τα ανθρώπινα λάθη και δομικές αστοχίες.
Οι κυβερνοεπιθέσεις που λαμβάνουν χώρα σε όλο τον κόσμο είναι όλο και περισσότερες και πιο εξελιγμένες και η ανάγκη για αποδοτική διαχείριση της πληροφορίας ως προς τις απειλές αυτές (Cyber Threat Intelligence – CTI) είναι μεγάλη. Για να μπορέσουν οι οργανισμοί να αναγνωρίσουν, να ταξινομήσουν και να ανταλλάξουν τα δεδομένα που σχετίζονται με τις κυβερνοαπειλές, χρειάζονται σαφώς δομημένα πλαίσια εννοιών και πληροφορίας.
Εδώ έρχονται οι οντολογίες, οι ταξινομίες και οι θησαυροί εννοιών, τα οποία αποτελούν εργαλεία για την αναπαράσταση και την οργάνωση της πληροφορίας. Ενώ οι σύνηθες προσεγγίσεις βασίζονται σε λίστες και ιεραρχίες, η χρήση προτύπων Σημασιολογικού Ιστού όπως το SKOS (Simple Knowledge Organization System) επιτρέπει την ομαδοποίηση και τη σύνδεση των εννοιών αυτών με τρόπο που μπορούν να υποστηρίξουν τίς ανάγκες στον τομέα της κυβερνοασφάλειας.

1.1 Σκοπός και στόχοι της εργασίας

Η παρούσα εργασία εξετάζει πώς το μοντέλο SKOS μπορεί να χρησιμοποιηθεί για τη δημιουργία μιας οντολογίας που θα ταξινομεί τις έννοιες του Cyber Threat Intelligence. Μέσα από αυτήν την προσέγγιση, παρουσιάζονται όροι και έννοιες που αφορούν απειλές, επιθέσεις, κακόβουλο λογισμικό και τακτικές που χρησιμοποιούνται στον κυβερνοχώρο από κακόβουλους συνήθως χρήστες. Παράλληλα, θα διερευνηθεί πώς αυτή η προσέγγιση μπορεί να συνδεθεί με υπάρχοντα πρότυπα όπως το MITRE ATT&CK και το STIX, ώστε να βελτιωθεί η διαλειτουργικότητα των πληροφοριακών συστημάτων στον χώρο της κυβερνοασφάλειας.
Στόχος της παρούσας είναι να γεφυρώσει το χάσμα μεταξύ των δεδομένων που συλλέγονται και της οργάνωσης στον κόσμο των μεταδεδομένων (metadata), προσφέροντας μια πρόταση που επιτρέπει την πιο αποδοτική ανάλυση και ανταλλαγή πληροφοριών. Οι τεχνολογίες του

σημασιολογικού ιστού, οι οντολογίες και οι ταξινομίες στον τομέα του CTI μπορούν να παρέχουν πολύτιμες πληροφορίες από την συλλογή δεδομένων που μπορεί να έχουν. Οι οντολογίες είναι ένα ώριμο πεδίο σημασιολογικών τεχνολογιών, και υπάρχουν διάφορες μεθοδολογίες, σχέδια και εργαλεία για την ανάπτυξή τους, καθώς και γλώσσες και τεχνολογίες όπως RDF, OWL, λογιστές και SPARQL. Μέσα από αυτή τη μελέτη, ευελπιστούμε να αναδείξουμε τη σημασία οντολογιών, ταξινομιών, θησαυρών στο CTI και να συμβάλουμε στη βελτίωση των πρακτικών διαχείρισης της πληροφορίας στον κυβερνοχώρο.

1.2 Δομή της εργασίας

Αρχικά, παρουσιάζεται το θεωρητικό υπόβαθρο, με ορισμούς και διακρίσεις ανάμεσα σε βασικές έννοιες όπως η οντολογία, η ταξινομία και οι θησαυροί. Στη συνέχεια, εξετάζεται το πεδίο του CTI, αναλύοντας τα βασικά πρότυπα που το συνοδεύουν, όπως τα STIX, TAXII και MITRE ATT&CK, καθώς και μοντέλα όπως το Diamond Model το DML και το CTI.

Ακολουθεί εκτενής αναφορά στο μοντέλο SKOS, περιγράφοντας τα βασικά χαρακτηριστικά του, τις ιδιότητες και τις κλάσεις που το απαρτίζουν, καθώς και τη συγκριτική του αποτίμηση σε σχέση με άλλα μοντέλα όπως το OWL ή τα παραδοσιακά συστήματα θησαυρών. Στη συνέχεια, παρουσιάζεται η πρακτική εφαρμογή του SKOS στην αναπαράσταση γνώσης στο CTI.

Στο τέταρτο κεφάλαιο, περιγράφεται αναλυτικά η μεθοδολογία που ακολουθήθηκε για την ανάπτυξη της οντολογίας στο λογισμικό Protege, από τον ορισμό των εννοιών έως τη διασύνδεσή τους και την εξαγωγή του αποτελέσματος. Τέλος, η εργασία ολοκληρώνεται με συμπεράσματα και προτάσεις για μελλοντικές βελτιώσεις, ενώ παρατίθεται και τεχνικό παράρτημα με συνοδευτικό κώδικα Python.

Συνολικά, η εργασία προσφέρει μια προσέγγιση στην εφαρμογή μοντέλων σημασιολογικού ιστού στο πεδίο της κυβερνοασφάλειας, με στόχο τη βελτίωση της αναπαράστασης, κατανόησης και ανταλλαγής γνώσης όσον αφορά τις κυβερνοαπειλές.

Κεφάλαιο 2ο: Θεωρητικό υπόβαθρο

2.1 Οντολογίες, Ταξινομίες και Θησαυροί

2.1.1 Οντολογία

Η λέξη οντολογία προέρχεται από τις δύο ελληνικές λέξεις όντος (όντος, που σημαίνει να είσαι) και λογία (λογία, που σημαίνει επιστήμη, μελέτη ή θεωρία) (Wikipedia 2010). Η οντολογία είναι η φιλοσοφική μελέτη της φύσης της ύπαρξης, της ύπαρξης ή της πραγματικότητας. Η οντολογία εστιάζει στο πώς μπορεί να αναπαρασταθεί η γνώση. Στόχος του είναι να προσδιορίσει ποιες οντότητες υπάρχουν και φιλοσοφεί για το πώς αυτές οι οντότητες μπορούν να ταξινομηθούν και/ή να σχετίζονται μεταξύ τους. Οι κανόνες και οι οντολογίες παίζουν βασικό ρόλο στην πολυεπίπεδη αρχιτεκτονική του Σημασιολογικού Ιστού, καθώς χρησιμοποιούνται για να αποδώσουν νόημα σε δεδομένα που βρίσκονται στον παγκόσμιο Ιστό και το επίπεδο οντολογίας που υπάρχει είναι αρκετά μεγάλο (Kourie 2014).

2.1.2 Ταξινομία

Η λέξη ταξινομία αναφέρεται στην επιστήμη της ταξινόμησης των πραγμάτων και παραδοσιακά αναφέρεται κυρίως στην ταξινόμηση των φυτών και των ζώων. Πρόκειται πλέον για ένα δημοφιλή όρο που αφορά οποιοδήποτε σύστημα ιεραρχικής ταξινόμησης ή κατηγοριοποίησης. Αυτό ισχύει περισσότερο πλέον στο χώρο των επιχειρήσεων. Έτσι η ταξινόμηση είναι ένα ελεγχόμενο λεξιλόγιο στο οποίο όλοι οι όροι ανήκουν σε μια ενιαία ιεραρχική δομή και συνδέονται άλλοτε στενότερα και άλλοτε ευρύτερα με άλλους όρους. Η δομή αναφέρεται μερικές φορές και ως ο κορμός πάνω στον οποίο προστίθενται τα μέρη μιας ταξινόμησης (Kourie 2014).

Μια ταξινόμηση δημιουργείται ομαδοποιώντας τα πράγματα σε έναν τομέα σε κατηγορίες και υποκατηγορίες. Συχνά οι υποκατηγορίες σχηματίζονται σε πολλά βαθύτερα επίπεδα. Όταν δύο έννοιες βρίσκονται σε μια ιεραρχική σχέση, η υπέρ-έννοια ονομάζεται υπέρ-ώνυμο της υπό-έννοιας και η υπό-έννοια ονομάζεται υπό-ώνυμο της υπέρ-έννοιας. Εξασφαλίζει τη μεταφορά ιδιοτήτων από υπέρ-έννοιες σε υπό-έννοιες. Μερικές φορές τίθενται περιορισμοί στα υπέρ-ώνυμα και τα υπό-ώνυμα στην ταξινόμηση. Ο Garshol (2004) περιγράφει την πολύπλευρη ταξινόμηση ως έναν πειθαρχημένο τρόπο κατασκευής ενός θησαυρού. Αντιθέτως, ονομάζουμε μια τέτοια πολύπλευρη ιεραρχική δομή ταξινόμηση επειδή έχει μόνο ιεραρχικές σχέσεις. Όταν κάθε έννοια περιορίζεται σε ένα μόνο υπέρ-ώνυμο, η ταξινόμηση είναι αυστηρά ιεραρχική και μπορεί να παρουσιαστεί σε δομή δέντρου. Σε μια τέτοια ταξινόμηση η θέση κάθε στοιχείου καθορίζεται μοναδικά καθώς κάθε στοιχείο μπορεί να ανήκει μόνο σε μία υποκατηγορία η οποία με τη σειρά της μπορεί να έχει μόνο μία υπέρ-κλάση. Εάν οι έννοιες επιτρέπεται να έχουν πολλαπλά υπέρ-ώνυμα, η δομή που προκύπτει είναι ένα ημί-πλέγμα όπως ορίζεται στη μαθηματική θεωρία πλέγματος (Birkhoff 1948; Wille 1982; Grätzer 2011). Ο Lambe (2007) τις αποκαλεί πολύ-ιεραρχίες (Kourie 2014).

Ενώ τα έγγραφα κειμένου μπορούν να μπουν σε ένα ευρετήριο αυτόματα ή να ταξινομηθούν αυτόματα με βάση ερωτήματα αναζήτησης που ταιριάζουν με λέξεις μέσα στα κείμενα, τα μη-γραπτά ψηφιακά αρχεία συνήθως απαιτούν κάποιου είδους περιγραφική σήμανση προκειμένου να ανακτηθούν σε αναζητήσεις θέματος. Η ανεξέλεγκτη προσθήκη ετικετών λέξεων-κλειδιών τείνει να είναι ασυνεπής, ανεπαρκής, πολύ γενική και μεροληπτική, οδηγώντας σε ανακριβή αποτελέσματα ανάκτησης. Η λύση για την δημιουργία ευρετηρίου είναι η εφαρμογή ελεγχόμενων λεξιλογίων σε περιγραφικά πεδία μεταδεδομένων.

Οι ταξινομίες ή αλλιώς τα ελεγχόμενα λεξιλόγια χρησιμοποιούνται σε περιγραφικά πεδία μεταδεδομένων για την υποστήριξη συνεπούς, ακριβούς και γρήγορης εύρεσης και ανάκτησης

περιεχομένου ψηφιακών στοιχείων. Ο σχεδιασμός μεταδεδομένων και ελεγχόμενων λεξιλογίων είναι μια ολοκληρωμένη διαδικασία που λαμβάνει υπόψη ποια και πόσα πεδία μεταδεδομένων θα χρησιμοποιήσουν τα ελεγχόμενα λεξιλόγια. Τα συνώνυμα (μη προτιμώμενοι όροι) και οι ιεραρχίες είναι μέθοδοι που βοηθούν τους χρήστες να βρουν τον σωστό όρο μέσα σε ένα μεγάλο ελεγχόμενο λεξιλόγιο. Επεξηγούνται οι βέλτιστες πρακτικές για τη δημιουργία μη προτιμώμενων όρων και ιεραρχιών. Ο σχεδιασμός των μεταδεδομένων για ψηφιακά στοιχεία αναπόφευκτα θέτει το ζήτημα των ελεγχόμενων λεξιλογίων, ταξινομιών, λέξεων-κλειδιών ή ετικετών.

2.1.3 Θησαυροί

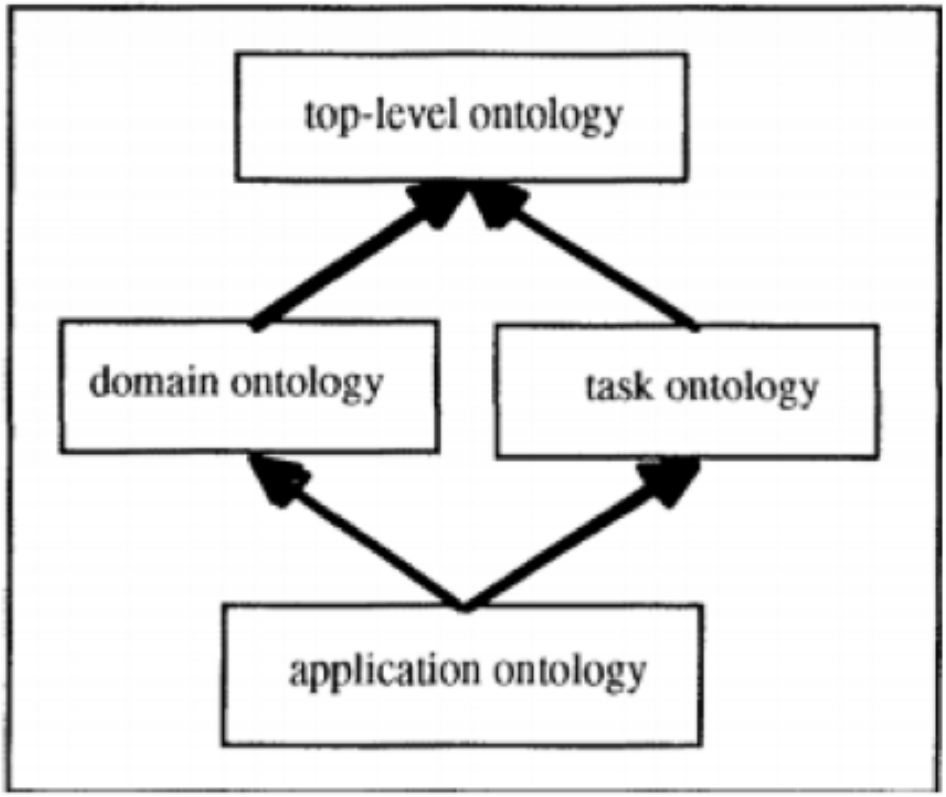
Η λέξη θησαυρός είναι μια λατινική λέξη που προκύπτει από τη λατινοποίηση της ελληνικής λέξης Θησαυρός (thesaurus, που σημαίνει αποθήκη θησαυρού) (Wikipedia 2011). Ο όρος, ωστόσο, σήμερα χρησιμοποιείται συχνότερα για να αναφέρεται σε μια ταξινομημένη λίστα όρων και των συνωνύμων τους σε ένα συγκεκριμένο πεδίο, , ένα λεξικό, εγκυκλοπαίδεια ή «αποθήκη» γνώσης. Αυτή η αλλαγή στο νόημα από μια συλλογή θησαυρού σε ένα λεξικό συνωνύμων έγινε με τη δημοσίευση του Θησαυρού των Αγγλικών Λέξεων και Φράσεων του Ro-get (1912). Πιθανότατα, η σημασία της λέξης θησαυρός σε αυτόν τον τίτλο επιλέχθηκε για να περιγράψει τη συλλογή ως μια πολύτιμη πηγή λέξεων και φράσεων για πρακτική εφαρμογή. Η δημοσίευση αυτή κυκλοφόρησε για πρώτη φορά το 1852, και ο Roget το περιέγραψε ως «ταξινομημένο κατάλογο λέξεων», χρησιμοποιήθηκε ευρέως και ο τίτλος του έγινε σταδιακά συνώνυμος με την πρόθεσή του, όπως η λέξη google χρησιμοποιείται σήμερα ως ρήμα συνώνυμο με την έννοια της αναζήτησης στο διαδίκτυο, προσφέροντας λειτουργίες αναζήτησης στο διαδίκτυο. Με άλλα λόγια ένας θησαυρός είναι μια συλλογή που περιέχει στοιχεία σε έναν επιλεγμένο τομέα. Ένας θησαυρός επιτρέπει τον προσδιορισμό των ιδιοτήτων των στοιχείων καθώς και τον ορισμό των σημασιολογικών σχέσεων ισοδυναμίας, ιεραρχικών, συνειρμικών και/ή αντίθεσης μεταξύ των στοιχείων του (Kourie 2014).

Αυτοί οι τρεις ορισμοί θα είναι γνωστοί σε πολλούς, αλλά και οι τρεις λέξεις έχουν πλέον οικειοποιηθεί και ανατραπεί από σύγχρονους εργαζόμενους στις επιστήμες της πληροφορίας. Στη διαδικασία, τείνει να υπάρχει, κατά καιρούς, μια σημαντική αλληλοεπικάλυψη, ακόμη και αντίφαση, στις τρεις λέξεις όπως χρησιμοποιούνται σήμερα. Δεν θα ήταν λογικό να επικαλεστούμε τις «σωστές» έννοιες αυτών των λέξεων, αλλά προσπαθώντας να οριοθετήσουμε τα κεντρικά χαρακτηριστικά αυτών των τριών όρων, ελπίζουμε ότι ο αναγνώστης θα κατανοήσει σαφέστερα τις διαφορές και τις ομοιότητές τους, καθώς και πώς θα μπορούσαν να αρχίσουν να χρησιμοποιούνται πιο στενά μεταξύ τους [2] (Gilchrist 2003).

2.2 Χρήση στην αναπαράσταση γνώσης

Οι οντολογίες, οι ταξινομίες και οι θησαυροί έχουν σημαντικό ρόλο στην αναπαράσταση της γνώσης, παρέχοντας την κατάλληλη δομή που διευκολύνουν την οργάνωση, την κατανόηση και την ανάκτηση πληροφοριών σε διάφορες περιοχές αναζήτησης. Οι οντολογίες χρησιμοποιούνται για την τυπική αναπαράσταση εννοιών και των σχέσεων τους εντός ενός πεδίου γνώσης. Αυτές οι δομές επιτρέπουν την κατανόηση και την ανταλλαγή πληροφορίας μεταξύ διαφορετικών οργανισμών, απλών χρηστών. Για παράδειγμα, στον Σημασιολογικό Ιστό, οι οντολογίες διευκολύνουν τη διαλειτουργικότητα ξεχωριστών εφαρμογών, επιτρέποντας την αυτόματη επεξεργασία και ερμηνεία των δεδομένων πληροφορίας από υπολογιστικά συστήματα. Επιπλέον, οι οντολογίες χρησιμοποιούνται στη μηχανική συστημάτων για την μετάφραση μεταξύ διαφορετικών γλωσσών και αναπαραστάσεων, διευκολύνοντας την επικοινωνία και τη διαλειτουργικότητα μεταξύ διαφορετικών τεχνολογιών.

Οι οντολογίες μπορούν να χωριστούν:



Εικόνα 1 - Kinds of ontologies, according to their level of dependence on a particular (https://www.loa.istc.cnr.it/old/Papers/FOIS98.pdf)

όπως παρουσιάζει ο Nicola Guarino σε τέσσερις (4) τύπους: ανώτατου επιπέδου, στον τομέα της εργασίας και στην εφαρμογή. Η σχέση εξειδίκευσης μεταξύ τους αντιπροσωπεύεται από τα βέλη που φαίνονται στο σχήμα Εικόνα 1. Οι ταξινομίες προσφέρουν μια ιεραρχική δομή που κατηγοριοποιεί έννοιες, πλαίσια ή αντικείμενα από ένα γενικό πεδίο σε ένα ειδικό. Αυτή η ιεραρχία διευκολύνει την οργάνωση και την ανάκτηση πληροφοριών, επιτρέποντας στους χρήστες να κατευθύνονται εύκολα ενδιάμεσα σε μεγάλο αριθμό δεδομένων. Για παράδειγμα, σε βιβλιοθήκες και αρχεία, οι ταξινομίες χρησιμοποιούνται για την κατηγοριοποίηση βιβλίων και εγγράφων, διευκολύνοντας την αναζήτηση και την εύρεση των πληροφοριών (Guarino 1998).

Οι θησαυροί είναι ελεγχόμενα λεξιλόγια που οργανώνουν όρους και έννοιες με βάση τις σημασιολογικές τους σχέσεις, όπως συνώνυμα, αντώνυμα και ιεραρχίες. Χρησιμοποιούνται κυρίως στη βιβλιοθηκονομία και την ανάκτηση πληροφορίας και την ακρίβειας των αναζητήσεων. Για παράδειγμα, ο Ελληνικός Θησαυρός Επιστημονικών Όρων παρέχει ένα ελεγχόμενο λεξιλόγιο για την περιγραφή και την αναζήτηση επιστημονικών όρων ή γενικά πληροφοριών, εξασφαλίζοντας τη συνέπεια στη χρήση όρων και διευκολύνοντας την εύρεση τους.

Συνολικά, η χρήση αυτών των εργαλείων στην αναπαράσταση γνώσης συμβάλλει στην αποτελεσματική οργάνωση, ανάκτηση και ανταλλαγή πληροφοριών, υποστηρίζοντας την κατανόηση και τη συνεργασία μεταξύ διαφορετικών συστημάτων και χρηστών.

2.3 Cyber Threat Intelligence (CTI)

2.3.1 Ορισμός και σημασία

Η συνεχώς αυξανόμενη συχνότητα και πολυπλοκότητα των κυβερνοεπιθέσεων καθιστούν απαραίτητη την ανάπτυξη αποτελεσματικών μηχανισμών προστασίας για οργανισμούς κάθε μεγέθους. Η ευφυΐα Κυβερνοαπειλών (Cyber Threat Intelligence - CTI) αποτελεί ένα εργαλείο που επιτρέπει στους επαγγελματίες της κυβερνοασφάλειας να εντοπίζουν, να κατανοούν και να προλαμβάνουν τις απειλές πριν αυτές προκαλέσουν σημαντικές επιπτώσεις. Με την αξιοποίηση κατάλληλων δεδομένων και ανάλυσης τεχνικών, το CTI συμβάλλει στην ενίσχυση της άμυνας των οργανισμών έναντι σε πολλών ειδών επιθέσεων, βελτιώνοντας τις διαδικασίες ανίχνευσης, απόκρισης και μετριασμού ή και εξάλειψης των κινδύνων.

Το Cyber Threat Intelligence αναφέρεται με αρκετές έννοιες: CTI είναι τα δεδομένα που συλλέγονται, υποβάλλονται σε επεξεργασία και αναλύονται για να κατανοήσουν τα κίνητρα, τους στόχους και τις συμπεριφορές μιας επίθεσης ενός απειλητικού παράγοντα. Μας δίνει τη δυνατότητα να λαμβάνουμε πιο γρήγορες, πιο ενημερωμένες αποφάσεις για την ασφάλεια που βασίζονται σε δεδομένα και να αλλάξουμε τη συμπεριφορά τους από αντιδραστική σε προληπτική για την καταπολέμηση των όποιων απειλητικών παραγόντων (Bromander 2017).

Μία άλλη είναι: το CTI παρέχεται ως λύση για βοήθεια στη λήψη αποφάσεων κατά την αντιμετώπιση θεμάτων που σχετίζονται με την ασφάλεια . Μπορεί να περιγραφεί εν συντομία ως η διαδικασία συλλογής, επεξεργασίας και ανταλλαγής πληροφοριών που είναι πολύτιμες για την ανάλυση και τον εντοπισμό πιθανών απειλών στον κυβερνοχώρο. Στο πλαίσιο του CTI, τα μη επεξεργασμένα ακατέργαστα δεδομένα που προέρχονται από πολυάριθμες πηγές κυβερνοασφάλειας, όπως αναφορές, εγχειρίδια και ιστότοποι, χρησιμοποιούνται ως δεδομένα και στη συνέχεια χρησιμοποιούνται προσεκτικά για την εξαγωγή μιας χρήσιμης γνώσης. Με την πρόσβαση στο διαθέσιμο CTI, οι μικρομεσαίες επιχειρήσεις έχουν την ευκαιρία να ενισχύσουν την προστασία της υποδομής τους και να μειώσουν το κόστος απόκτησης σχετικών δεδομένων προκειμένου να μοιράζονται, να διανέμουν και να χρησιμοποιούν αποτελεσματικά πληροφορίες (Charalampos Bratsas and Lazaros Ioannidis 2024).

Κατανοώντας τα προαναφερόμενα μπορούμε να υιοθετήσουμε τον παρακάτω ορισμό:

<u>*Ορισμός*</u>:

Το Cyber Threat Intelligence αναφέρεται ως το έργο της συλλογής τεκμηριωμένων γνώσεων, συμπεριλαμβανομένων πλαισίου, μηχανισμών, δεικτών, επιπτώσεων και συμβουλών σχετικά με μια υπάρχουσα ή αναδυόμενη απειλή ή κίνδυνο για περιουσιακά στοιχεία που μπορούν να χρησιμοποιηθούν για την ενημέρωση αποφάσεων σχετικά με την απάντηση του υποκειμένου σε αυτήν την απειλή ή κίνδυνο.

Ως αποτέλεσμα, οι προμηθευτές πληροφοριών απειλών στρέφονται όλο και περισσότερο σε τρόπους αυτοματοποίησης αυτής της διαδικασίας καθιστώντας την ανάλυση απειλών μια βιώσιμη εργασία. Πλέον είναι αποδεδειγμένο ότι η ευφυΐα απειλών αποτελεί προτεραιότητα στις επιχειρήσεις κυβερνοασφάλειας κάθε οργανισμού που γνωρίζει την ασφάλεια ως τρόπος αποτροπής μιας επίθεσης ή μείωσης του χρόνου που απαιτείται για την ανακάλυψη μιας επίθεσης. Επιπλέον, οι επιθέσεις στον κυβερνοχώρο γίνονται όλο και πιο εξελιγμένες, θέτοντας σημαντικές προκλήσεις για τους οργανισμούς που πρέπει να υπερασπιστούν τα δεδομένα και τα συστήματά τους από ικανούς παράγοντες απειλών. Οι φορείς απειλών μπορεί να είναι επίμονοι, παρακινημένοι και ευέλικτοι και χρησιμοποιούν μια ποικιλία τακτικών, τεχνικών και διαδικασιών για να διαταράξουν το απόρρητο, την ακεραιότητα και τη διαθεσιμότητα συστημάτων και δεδομένων (Josang 2018).

Για να επιτύχει το CTI εντός του τομέα του κυβερνοχώρου απαιτεί μια γνωσιακή βάση πληροφοριών των απειλών και έναν εκφραστικό τρόπο αναπαράστασης αυτής της γνώσης. Αυτός ο σκοπός εξυπηρετείται με τη χρήση ταξινομιών, προτύπων κοινής χρήσης, θησαυρών και οντολογιών.

Το μοντέλο Πληροφοριών Κυβερνοαπειλής (CTI), επιτρέπει στους υπερασπιστές του κυβερνοχώρου να εξερευνήσουν τις δυνατότητές τους στον τομέα των πληροφοριών απειλών και να κατανοήσουν τη θέση τους απέναντι στο διαρκώς μεταβαλλόμενο τοπίο απειλών στον κυβερνοχώρο. Ως επί των πλείστων, χρησιμοποιούμε το μοντέλο για να αναλύσουμε και να αξιολογήσουμε αρκετές υπάρχουσες ταξινομίες, πρότυπα κοινής χρήσης και οντολογίες που σχετίζονται με νοημοσύνη των απειλών στον κυβερνοχώρο, όπου θα τα δούμε και ποιο κάτω στην αναφορά μας (Bromander 2017).

2.3.2 Βασικές έννοιες και πρότυπα (π.χ. STIX, TAXII, MITRE ATT&CK)

Στον τομέα του Cyber Threat Intelligence, έχουν αναπτυχθεί διάφορα πρότυπα και πλαίσια που διευκολύνουν τη συλλογή, ανάλυση και ανταλλαγή πληροφοριών απειλών.

STIX (Structured Threat Information eXpression)

Το STIX είναι μια γλώσσα και μια μορφή σειριοποίησης των δεδομένων και χρησιμοποιείται για την ανταλλαγή πληροφοριών για τις απειλές που μπορεί να υπάρχουν στον κυβερνοχώρο (CTI). Το STIX είναι ανοιχτού κώδικα και δωρεάν, επιτρέποντας στους ενδιαφερόμενους να το χρησιμοποιούν με δομημένο τρόπο και υποστηρίζει μία πιο αποτελεσματική διαχείριση των απειλών στον κυβερνοχώρο με διάφορες διαδικασίες αυτοματισμού κατά την εφαρμογή του (Open 2017-2024).

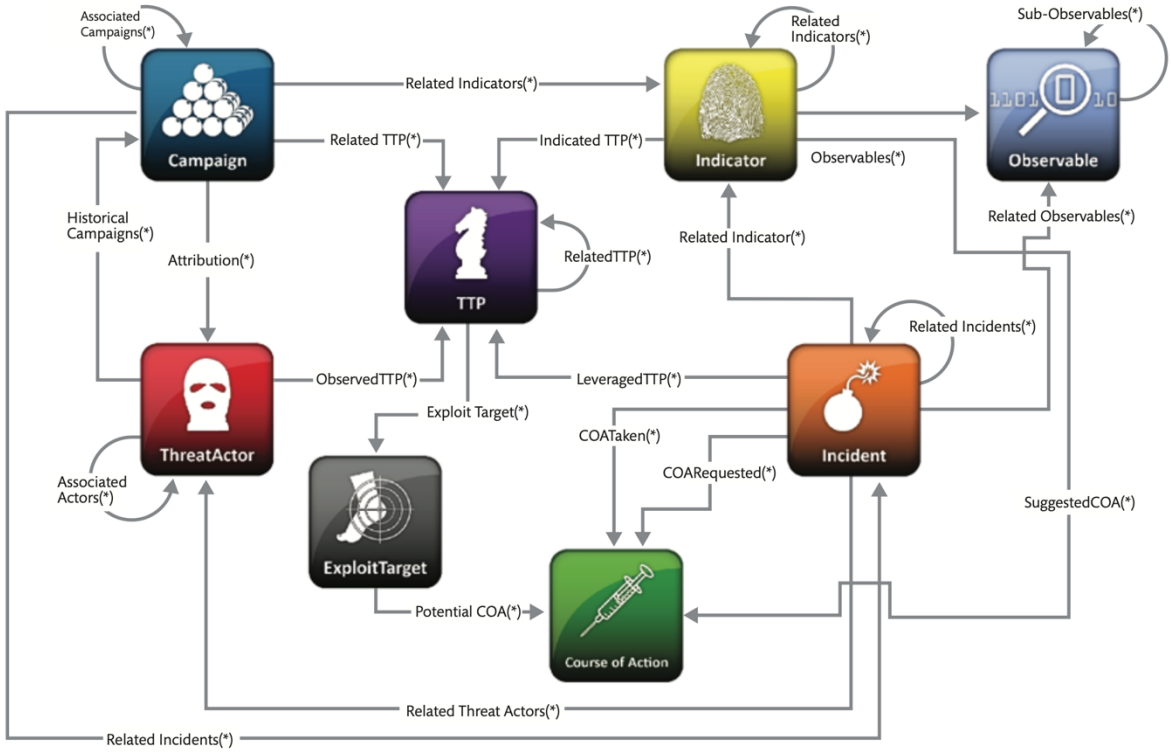
Μια ποικιλία περιπτώσεων χρήσης στην κυβερνοασφάλεια υψηλού επιπέδου που βασίζονται σε τέτοιες πληροφορίες μπορεί να είναι:

- Ανάλυση κυβερνοαπειλών (Analyzing cyber threats).
- Καθορισμός προτύπων δεικτών για τις απειλές στον κυβερνοχώρο (Pacifying Indicator Patterns for cyber threat).
- Διαχείριση δραστηριοτήτων αντιμετώπισης απειλών στον κυβερνοχώρο (Managing cyber threat response activities).
- Κοινή χρήση πληροφοριών για απειλές στον κυβερνοχώρο (Barnum 2014).

Επιπλέον, το STIX παρέχει μια ενοποιημένη αρχιτεκτονική που συνδέει ένα σύνολο ποικίλων απειλών στον κυβερνοχώρο, όπως πληροφορίες που περιλαμβάνουν (Barnum 2014):

- Παρατήρηση κυβερνοχώρου (Cyber Observables).
- Δείκτες (Indicators).
- Περιστατικά (Incidents).
- Τακτικές, τεχνικές και διαδικασίες (TTPs συμπεριλαμβανομένων μοτίβων επιθέσεων, κακόβουλου λογισμικού, εκμεταλλεύσεων, θανάτωσης αλυσίδες, εργαλεία, υποδομές, στόχευση θυμάτων κ.λπ.)
- Στόχοι εκμετάλλευσης (Exploit Targets, π.χ. τρωτά σημεία, αδυναμίες ή διαμορφώσεις)
- Μαθήματα Δράσης (Courses of Action, π.χ. απόκριση σε περιστατικό ή διορθώσεις ευπάθειας/αδυναμίας ή μετριασμούς)
- Εκστρατείες κυβερνοεπιθέσεων (Cyber Attack Campaigns).
- Συντελεστές Κυβερνοαπειλών (Cyber Threat Actors).

Την αρχιτεκτονική μπορούμε να την δούμε και παρακάτω στο σχήμα 2:

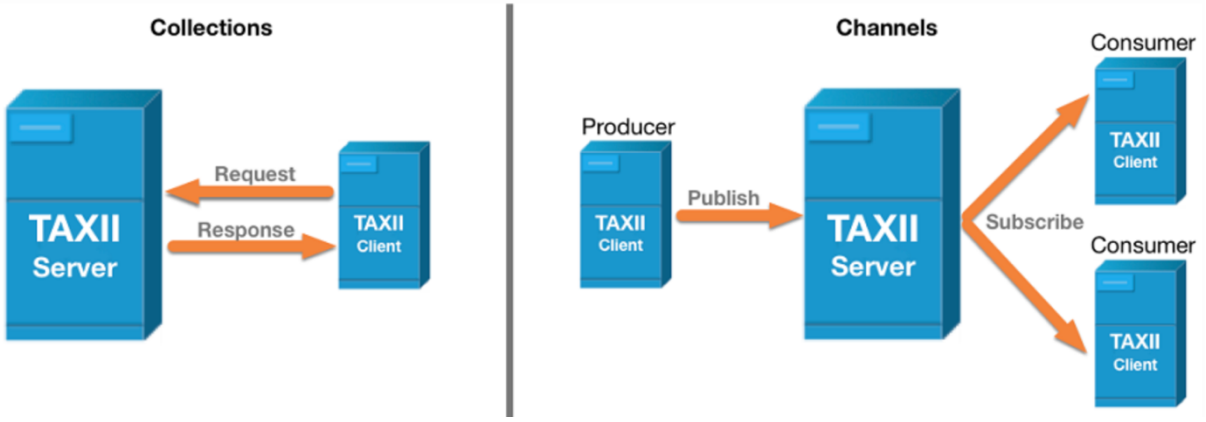


Εικόνα 2 - STIX Architecture [https://oasis-open.github.io/cti-documentation/stix/intro].

TAXII (Trusted Automated Exchange of Indicator Information)
Ένα πρωτόκολλο που χρησιμοποιείται για την ασφαλή και αυτοματοποιημένη ανταλλαγή πληροφοριών κυβερνοαπειλών μεταξύ οργανισμών μέσω HTTPS για την ασφαλή μεταφορά τους μέσω δικτύων. Ορίζεται ως ένα σύνολο υπηρεσιών ανταλλαγής μηνυμάτων και ένα σύνολο απαιτήσεων μεταξύ «πελατών» και Διακομιστή TAXII. Αυτές οι πληροφορίες μπορεί να περιλαμβάνουν διευθύνσεις IP, email, ονόματα παρόχων (Domains), καθώς και κακόβουλο λογισμικό (malware) που εντοπίζουν τρωτά σημεία ή και τρόπους άμυνας έναντι αυτών (Eric W. Burger 2014).
Το TAXII αποτελείται από δύο κύριες υπηρεσίες για την υποστήριξη μιας ποικιλίας κοινών μοντέλων κοινής χρήσης:

- Collections - Μια συλλογή ή διεπαφή μιας αποθήκης πληροφοριών CTI που μεταβιβάζονται από έναν διακομιστή (server) TAXII και επιτρέπει στους παρόχους να φιλοξενούν ένα σύνολο δεδομένων CTI που μπορούν πελάτες και Διακομιστές TAXII να ανταλλάσσουν πληροφορίες.
- Channels – Ένα κανάλι που επιτρέπει στους παρόχους να προωθούν δεδομένα σε πολλούς πελάτες και οι πελάτες να λαμβάνουν δεδομένα από πολλούς παρόχους αντίστοιχα. Οι πελάτες TAXII ανταλλάσσουν πληροφορίες με άλλους πελάτες TAXII σε ένα μοντέλο δημοσίευσης-εγγραφής.

Να σημειωθεί πως η έκδοση TAXII 2.1 διατηρεί τις λέξεις-κλειδιά που απαιτούνται για τα κανάλια, αλλά δεν καθορίζει τις υπηρεσίες του ίδιου του καναλιού (Open 2017-2024).
Στην εικόνα 3 που ακολουθεί, αποτυπώνεται το μοντέλο των υπηρεσιών TAXII:



Εικόνα 3 - TAXII sharing models

MITRE ATT&CK

Το MITRE ATT&CK είναι μία παγκοσμίου επιπέδου προσβάσιμη από όλους βάση γνώσης τακτικών και τεχνικών που βασίζονται σε πραγματικές παρατηρήσεις. Η βάση γνώσεων ATT&CK χρησιμοποιείται ως βάση για την ανάπτυξη συγκεκριμένων μοντέλων και μεθοδολογιών κυβερνοαπειλών σε ιδιωτικό , ομοσπονδιακό και σε κοινοτικό επίπεδο δεδομένων και υπηρεσιών στον κυβερνοχώρο (ATT&CK 2015-2024).
Ένα πλαίσιο που καταγράφει και κατηγοριοποιεί τις τακτικές, τεχνικές και διαδικασίες (TTPs) που χρησιμοποιούν οι επιτιθέμενοι, επιτρέποντας στους αναλυτές να κατανοήσουν και να μοντελοποιήσουν πιθανές επιθέσεις. Αυτά τα πρότυπα επιτρέπουν τη βελτίωση της συνεργασίας μεταξύ οργανισμών και την αποτελεσματικότερη ανταπόκριση στις κυβερνοαπειλές. Η αξιοποίησή τους συμβάλλει στη δημιουργία ενός ενιαίου και διαλειτουργικού συστήματος κυβερνοασφάλειας, όπου οι πληροφορίες μοιράζονται, διανέμονται και χρησιμοποιούνται αποτελεσματικά στην πρόληψη και αντιμετώπιση κυβερνοεπιθέσεων επιθέσεων.
Δραστηριοποιείται μεταξύ άλλων, στην έρευνα για την κυβερνοασφάλεια, έχοντας συμβάλει σημαντικά στη δημιουργία και διατήρηση βάσεων γνώσης σχετικών με το πεδίο αυτό. Πολλές από αυτές έχουν υιοθετηθεί ευρέως από όλη την κοινότητα της κυβερνοασφάλειας. Ένα χαρακτηριστικό παράδειγμα είναι το Common Vulnerabilities and Exposures (CVE), ένα πρότυπο που χρησιμοποιείται για την κατηγοριοποίηση και καταγραφή ευπαθειών λογισμικού, προσφέροντας ένα κοινό πλαίσιο αναφοράς για ειδικούς και οργανισμούς ασφαλείας. Υπάρχουν και άλλες ταξινομίες της MITRE μεταξύ άλλων που περιγράφουν τη συμπεριφορά των απειλών, όπως είναι το Common Attack Pattern Enumeration and Classification (CAPEC. Το CAPEC εστιάζει στην εκμετάλλευση ευπαθειών λογισμικού και παρέχει ένα σύνολο προτύπων επιθέσεων με σκοπό τη βελτίωση της ασφάλειας του λογισμικού. Το ATT&CK, από την άλλη, επικεντρώνεται στη συμπεριφορά των επιτιθέμενων και στο πώς αυτοί δρουν μέσα σε ένα δίκτυο, βοηθώντας στη βελτίωση της ασφάλειας των συστημάτων και των οργανισμών. Τα μοτίβα επιθέσεων που καταγράφονται στο CAPEC μπορούν να χρησιμοποιηθούν ως μέρος των τεχνικών που περιγράφονται στο ATT&CK, δημιουργώντας έτσι μια ενιαία προσέγγιση στην ανάλυση κυβερνοαπειλών. Και τα δύο μοντέλα έχουν σχεδιαστεί με γνώμονα την οπτική του επιτιθέμενου, ώστε να βοηθούν στην κατανόηση και αντιμετώπιση των επιθέσεων με πιο στοχευμένο τρόπο (Grønberg 2019).

2.4 Μοντέλα στο Cyber Threat Intelligence

Στον τομέα της κυβερνοασφάλειας, η κατανόηση και ανάλυση των κυβερνοαπειλών χρειάζεται καλά δομημένα μοντέλα CTI. Αυτά τα μοντέλα επιτρέπουν στους αναλυτές να κατηγοριοποιούν τις απειλές, να αναγνωρίζουν τα διάφορα μοτίβα επιθέσεων που δέχονται και να βελτιστοποιούν την ανίχνευση αυτών και την απόκριση σε αυτές.

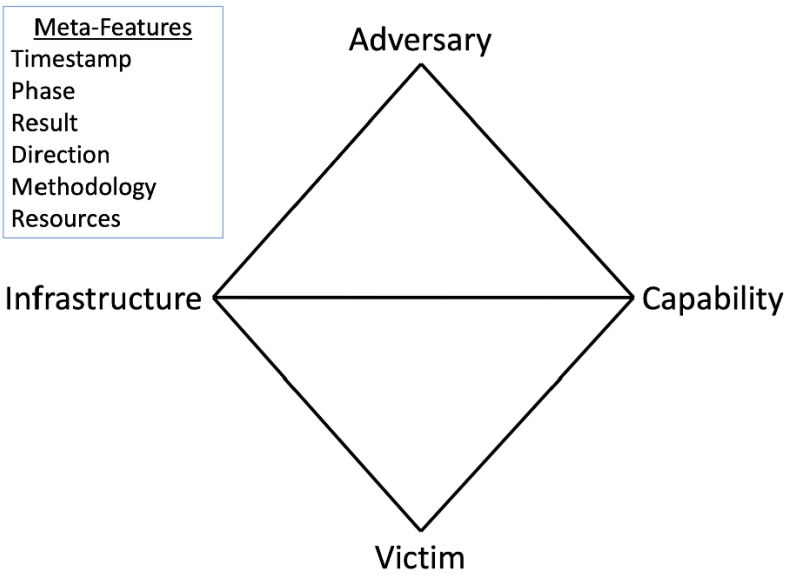
Στην παρούσα ενότητα, παρουσιάζονται τέσσερα από τα πιο σημαντικά μοντέλα που συμβάλλουν στην κατανόηση, κατηγοριοποίηση και ανάλυση των κυβερνοαπειλών:

- The Diamond Model of Intrusion Analysis: Ένα μοντέλο που αναλύει τα βασικά μοτίβα ενός περιστατικού εισβολής, εστιάζοντας στις σχέσεις μεταξύ επιτιθέμενου, θύματος, ικανοτήτων και υποδομών (Sergio Caltagirone).
- The Cyber Kill Chain: Ένα ιεραρχικό μοντέλο με φάσεις επίθεσης, το οποίο περιγράφει τα στάδια που ακολουθούνται από την αναγνώριση στόχου μέχρι και την τελική ολοκλήρωση της επίθεσης.
- The Detection Maturity Level (DML) Model: Ένα πλαίσιο που αξιολογεί την αποτελεσματικότητα των αμυντικών μηχανισμών ενός οργανισμού, με βάση το επίπεδο και τον τύπο των δεδομένων που χρησιμοποιούνται για την ανίχνευση κυβερνοεπιθέσεων.
- The Cyber Threat Intelligence (CTI) Model: Ένα μη ιεραρχικό μοντέλο που συνδυάζει τις έννοιες του DML με επιπλέον στοιχεία, προκειμένου να χαρακτηρίσει την ποιότητα και τη χρησιμότητα των πληροφοριών των επερχόμενων απειλών.

Κάθε ένα από αυτά τα μοντέλα προσφέρει μια διαφορετική οπτική στην κυβερνοασφάλεια, είτε εστιάζοντας στον τρόπο ανάλυσης των επιθέσεων, είτε στον τρόπο ανίχνευσης και αξιοποίησης των πληροφοριών. Στη συνέχεια, θα παρουσιαστούν αναλυτικά οι αρχές και οι εφαρμογές για το κάθε μοντέλο.

2.4.1 The Diamond Model of Intrusion Analysis

Το συγκεκριμένο μοντέλο προτάθηκε το 2013 από τους Sergio Caltaginore, Andrew Pendergast και Christopher Betz και από τότε είναι πολύ διαδεδομένο και χρησιμοποιούμενο μοντέλο στην ασφάλεια του κυβερνοχώρου, που αναλύει τα βασικά μοτίβα ενός περιστατικού εισβολής, εστιάζοντας στις σχέσεις μεταξύ επιτιθέμενου, θύματος, ικανοτήτων και υποδομών. Οι σχέσεις μεταξύ αυτών των τεσσάρων χαρακτηριστικών σχηματίζουν ένα ρόμβο που μοιάζει με διαμάντι όπως φαίνεται και στο παρακάτω σχήμα:



Εικόνα 4 - The Diamond Model of Intrusion Analysis (Sergio Caltagirone).

Για την οργάνωση και ανάλυση αυτών των συμβάντων, χρησιμοποιούνται χαρακτηριστικά (Meta-Features), τα οποία βοηθούν στην ταξινόμηση των γεγονότων, τη σύγκριση παρόμοιων συμβάντων και την καταγραφή κρίσιμων πληροφοριών. Τα βασικά χαρακτηριστικά περιλαμβάνουν:

- Χρονική σήμανση (Timestamp): Καταγράφει τη χρονική στιγμή έναρξης και λήξης του γεγονότος-συμβάντος ή επίθεσης.
- Φάση (Phase): Προσδιορίζει σε ποιο στάδιο της επίθεσης ανήκει το συμβάντος.
- Αποτέλεσμα (Result): Αναλύει το αποτέλεσμα του συμβάντος.
- Κατεύθυνση (Direction): Δείχνει αν η επίθεση ήταν εισερχόμενη ή εξερχόμενη.
- Μεθοδολογία (Methodology): Περιγράφει τον τρόπο εκτέλεσης της επίθεσης-συμβάντος.
- Πόροι (Resources): Περιλαμβάνει τα μέσα και τις τεχνικές που χρησιμοποιήθηκαν.

Τα βασικά χαρακτηριστικά και meta - χαρακτηριστικά πρέπει να υπάρχουν σε κάθε συμβάν, καθιστώντας το μοντέλο ιδιαίτερα χρήσιμο για την αναγνώριση κενών γνώσης σχετικά με τις κυβερνοαπειλές. Πλεονέκτημα αυτού του μοντέλου είναι ότι παρέχει μια αποτελεσματική όχι όμως και απαραίτητα ολοκληρωμένη λίστα χαρακτηριστικών που πρέπει να υπάρχουν σε κάθε εκδήλωση μίας επίθεσης. Επομένως, μετά την ανάλυση-τεκμηρίωση ενός συμβάντος με όλες τις διαθέσιμες πληροφορίες τυχόν κενά χαρακτηριστικά, εντοπίζονται πλέον και κενά γνώσης τα οποία θα πρέπει να γίνει σχετική αντίστροφη διαδικασία για να καλυφθούν αυτά τα κενά. Παρόλο που το μοντέλο δεν αποτελεί οντολογία από μόνο του, οι δημιουργοί του το προτείνουν ως θεμέλιο για την ανάπτυξη μιας οντολογίας, όπως αναφέρεται και σε άλλες μελέτες. Κάθε χαρακτηριστικό ενός συμβάντος στο μοντέλο περιλαμβάνει μια τιμή εμπιστοσύνης (confidence value), η οποία δεν είναι προκαθορισμένη αλλά μπορεί να προσαρμοστεί ανάλογα με την εκάστοτε εφαρμογή ανάπτυξης (Sergio Caltagirone).

2.4.2 The Cyber Kill Chain

Το Cyber Kill Chain μοντέλο ή γνωστό και ως Intelligence-driven Computer Network Defense, προτάθηκε από τους ερευνητές της Lockheed Martin εταιρίας και περιγράφει τις φάσεις από την στιγμή της επίθεσης, δηλαδή αναλύει την επίθεση ως ένα σταδιακό γεγονός. Κάθε ένα από τα στάδια μπορούν να ανιχνευθούν και να αναλυθούν και αυτές οι πληροφορίες που προκύπτουν μπορούν να αξιοποιηθούν βοηθώντας στην πρόληψη παρέχοντας μία ασφάλεια (Flaborea 2024).

Στον τομέα της κυβερνοασφάλειας, ο κίνδυνος μπορεί να θεωρηθεί σε συνάρτηση της πιθανότητας εκμετάλλευσης μιας ευπάθειας από μια απειλή και του αντίκτυπου που αυτή θα έχει στον στόχο. Σύμφωνα με τη Lockheed Martin, ενώ έχουν γίνει σημαντικές προσπάθειες για τον περιορισμό των ευπαθειών, δεν έχει δοθεί ανάλογη έμφαση στον περιορισμό του παράγοντα απειλή. Έτσι, ανέπτυξαν αυτό το μοντέλο, βασισμένο στη συλλογή πληροφοριών (intelligence-driven defense) που βοηθά στην αντιμετώπιση της εισβολής σε συνάρτηση με τον κίνδυνο.

Το Cyber Kill Chain αναλύει τη διαδικασία μιας κυβερνοεπίθεσης σε επτά διαδοχικές φάσεις:

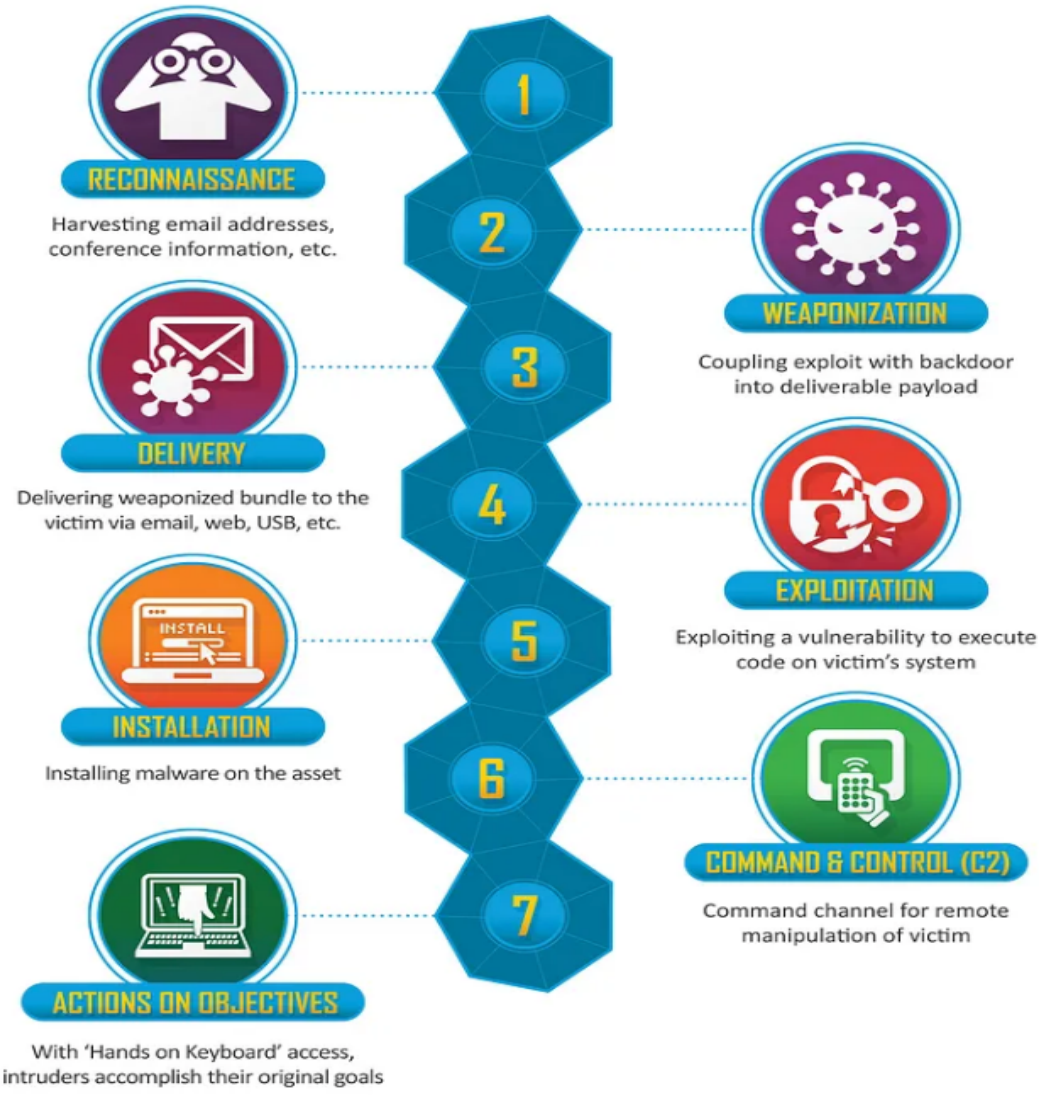
1. Reconnaissance (Αναγνώριση)
   Ο επιτιθέμενος αναγνωρίζει τον στόχο και συλλέγει πληροφορίες για αυτόν (π.χ. μέσω scanning, OSINT, social engineering).
2. Weaponization (Όπλιση)
   Δημιουργείται το κακόβουλο payload, το οποίο περιλαμβάνει έναν απομακρυσμένο trojan (RAT) ή άλλο exploit.
3. Delivery (Παράδοση)
   Το κακόβουλο λογισμικό παραδίδεται στο θύμα μέσω email, μολυσμένων ιστοσελίδων, USB ή άλλων μεθόδων.
4. Exploitation (Εκμετάλλευση)

Το κακόβουλο λογισμικό εκτελείται στο σύστημα του θύματος, εκμεταλλευόμενο ευπάθειες λογισμικού ή λειτουργικού συστήματος.

5. Installation (Εγκατάσταση)
   Ο επιτιθέμενος εγκαθιστά ένα backdoor ή ένα RAT για να εξασφαλίσει παρατεταμένη πρόσβαση στο σύστημα του θύματος.
6. C2 (Command & Control – Εντολές και Έλεγχος)
   Δημιουργείται ένα κανάλι επικοινωνίας μεταξύ του μολυσμένου συστήματος και του επιτιθέμενου, μέσω του οποίου εκτελούνται εντολές απομακρυσμένου ελέγχου.
7. Actions on Objectives (Ενέργειες στον Στόχο)
   Ο επιτιθέμενος χρησιμοποιεί την πρόσβαση που απέκτησε για να επιτύχει τους στόχους της επίθεσης, όπως:

- Κλοπή δεδομένων (data exfiltration)
- Πλάγια μετακίνηση σε άλλα συστήματα (lateral movement)
- Αλλοίωση δεδομένων (data manipulation)

Στο παρακάτω σχήμα φαίνονται τα στάδια του μοντέλου:

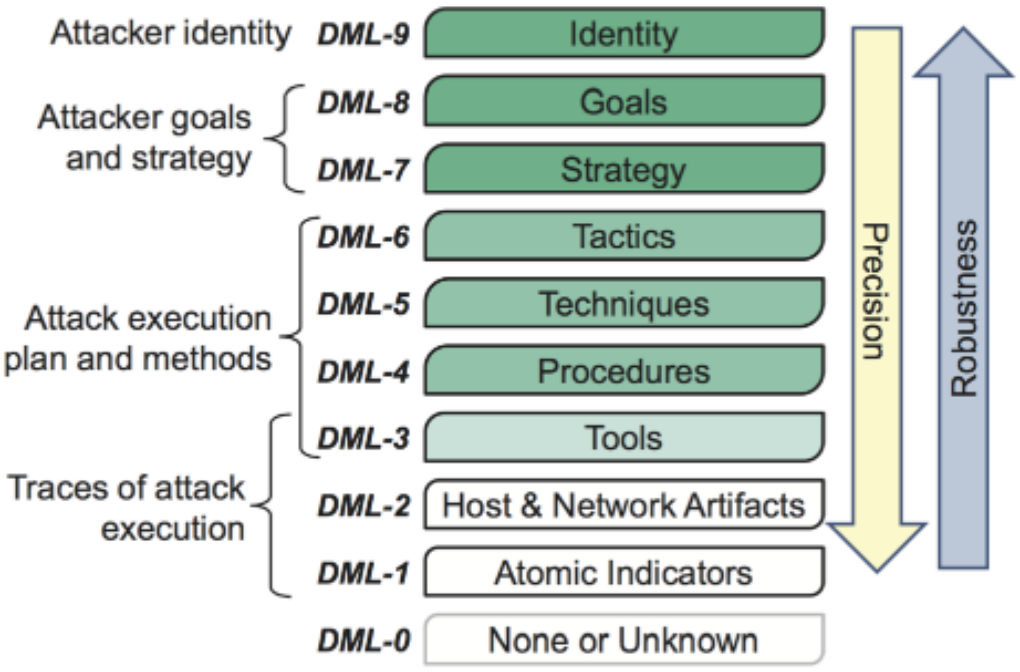


Εικόνα 5 - The Cyber Kill Chain (https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html)

Η διαδικασία μιας κυβερνοεπίθεσης ονομάζεται "αλυσίδα" επειδή αν αποτραπεί ή ανιχνευθεί σε ένα στάδιο, τότε διακόπτεται ολόκληρη η επίθεση. Για παράδειγμα, αν ένας οργανισμός εντοπίσει και μπλοκάρει ένα κακόβουλο email στη φάση Delivery, τότε τα επόμενα στάδια της αλυσίδας δεν θα εκτελεστούν.
Το μοντέλο αναδεικνύει μια ασυμμετρία μεταξύ επιτιθέμενου και αμυνόμενου όπου οποιοδήποτε στοιχείο επαναλαμβάνει ο επιτιθέμενος μπορεί να μετατραπεί σε αδυναμία. Η ανάλυση της φύσης αυτής της επανάληψης είτε προκύπτει από ευκολία, προσωπική προτίμηση ή άγνοια, μπορεί να βοηθήσει στην αξιολόγηση του κόστους των επιθέσεων. Η μοντελοποίηση της σχέσης κόστους-οφέλους για τους εισβολείς αποτελεί ένα πεδίο περαιτέρω έρευνας. Όταν το κόστος της επίθεσης γίνει δυσανάλογα υψηλό σε σχέση με το όφελος, αυτό μπορεί να υποδηλώνει ότι ένας οργανισμός έχει αποκτήσει πληροφοριακή υπεροχή έναντι των επιτιθέμενων. Το Cyber Kill Chain προσφέρει ένα δομημένο πλαίσιο στην ανάλυση των κυβερνοεπιθέσεων, βοηθώντας τους οργανισμούς να εντοπίσουν ευπάθειες και να ενισχύσουν την άμυνά τους σε κάθε στάδιο. Αντί να εστιάζουν μόνο στην επιδιόρθωση των ευπαθειών τους, μπορούν να παρέμβουν στην αλυσίδα, αυξάνοντας το κόστος για τον επιτιθέμενο και μειώνοντας τις πιθανότητες επιτυχίας μιας επίθεσης (Eric M. Hutchins 2011).

2.4.3 The Detection Maturity Level (DML)

Ο Ryan Stillions πρότεινε το Detection Maturity Level (DML) Model σε μια σειρά άρθρων στο προσωπικό του blog post το 2014. Το μοντέλο αρχικά σχεδιάστηκε για να περιγράψει την ωριμότητα ενός οργανισμού σε σχέση με την ικανότητά του να λαμβάνει και να αξιοποιεί πληροφορίες κυβερνοαπειλών. Αυτές οι πληροφορίες μπορεί να περιλαμβάνουν Indicators of Compromise (IoCs), Τακτικές, Τεχνικές και Διαδικασίες των επιτιθέμενων (TTPs), αναφορές κυβερνοαπειλών, και πολλά άλλα δεδομένα σχετιζόμενα με την ασφάλεια στον κυβερνοχώρο. Το 2016, το μοντέλο επεκτάθηκε με την προσθήκη ενός επιπλέον επιπέδου (Level 9 - "Identity"), με στόχο να χρησιμοποιηθεί για τη σημασιολογική αναπαράσταση των κυβερνοαπειλών στο διαδίκτυο (Stillions 2014).
Στην παρακάτω εικόνα φαίνεται η Δομή του μοντέλου:



Εικόνα 6 - The Detection Maturity Level Model (Bromander 2017).

Τα ανώτερα επίπεδα του μοντέλου περιλαμβάνουν:

- DML-8: Goals και DML-7: Strategy, τα οποία αφορούν τους γενικούς στόχους και τις στρατηγικές που χρησιμοποιούν οι επιτιθέμενοι. Αυτές οι πληροφορίες είναι συχνά δύσκολα μπορούν να χρησιμοποιηθούν για άμεση ανίχνευση των επιθέσεων αλλά η χρήση σημασιολογικών τεχνολογιών θα μπορούσε να βοηθήσει στην αναπαράστασή τους.

Τα επόμενα τρία επίπεδα επικεντρώνονται στις τακτικές και μεθόδους των επιτιθέμενων:

- DML-6: Tactics - Περιγράφουν τι κινήσεις πραγματοποιεί ο επιτιθέμενος κατά τη διάρκεια μιας επίθεσης.
- DML-5: Techniques - Περιγράφουν συγκεκριμένους τρόπους με τους οποίους πραγματοποιούνται οι επιθέσεις.
- DML-4: Procedures - Αναφέρονται στο πώς εκτελείται μια επίθεση, ποια βήματα ακολουθούνται και με ποια σειρά.

Ο Ryan Stillions, σε ένα από τα άρθρα του, εξηγεί τη διαφορά μεταξύ Tactics, Techniques & Procedures (TTPs):

Οι τακτικές (tactics) είναι πιο γενικές και λιγότερο τεχνικές από τις τεχνικές. Οι τεχνικές (techniques) είναι πιο τεχνικές αλλά λιγότερο συγκεκριμένες από τις διαδικασίες. Οι διαδικασίες (procedures) περιγράφουν με ακριβή και προδιαγεγραμμένο τρόπο τα βήματα που ακολουθεί ένας επιτιθέμενος. Δεδομένου ότι πολλοί από τους επιτιθέμενους, επαναλαμβάνουν τα ίδια βήματα στις επιθέσεις τους, η ανίχνευση με βάση τις διαδικασίες (procedures) αποτελεί σημαντική βελτίωση για τους περισσότερους οργανισμούς (Stillions 2014).

Η ανίχνευση σε DML-3 (Tools) βασίζεται στην ανίχνευση των εργαλείων που χρησιμοποιούνται για την ανίχνευση μιας επίθεσης. Αυτό μπορεί να περιλαμβάνει την παρακολούθηση της μεταφοράς, της παρουσίας ή της λειτουργίας ενός εργαλείου σε ένα σύστημα. Όμως, όσο ένας οργανισμός προχωρά από το DML-3 προς τα ανώτερα επίπεδα, η ανίχνευση μετακινείται από την παρακολούθηση αυτών των εργαλείων προς την ανάλυση της συμπεριφοράς του επιτιθέμενου.

Οι Χαμηλότερες Βαθμίδες του μοντέλου:

- DML-2: Host & Network Artifacts - Δείκτες που παρατηρούνται κατά τη διάρκεια ή μετά το πέρας μιας επίθεσης, όπως αρχεία καταγραφής συστήματος, κακόβουλες συνδέσεις δικτύου, ή αρχεία που δημιουργούνται από κακόβουλο λογισμικό (malware).
- DML-1: Atomic Indicators - Τα μικρότερα, ανεξάρτητα στοιχεία μιας απειλής, όπως IP διευθύνσεις, domain ή hashes αρχείων.

Αυτά τα δεδομένα έχουν πολύ μικρό χρόνο ζωής, καθώς οι επιτιθέμενοι μπορούν εύκολα να αλλάξουν τις διευθύνσεις ή τις υπογραφές των κακόβουλων αρχείων.

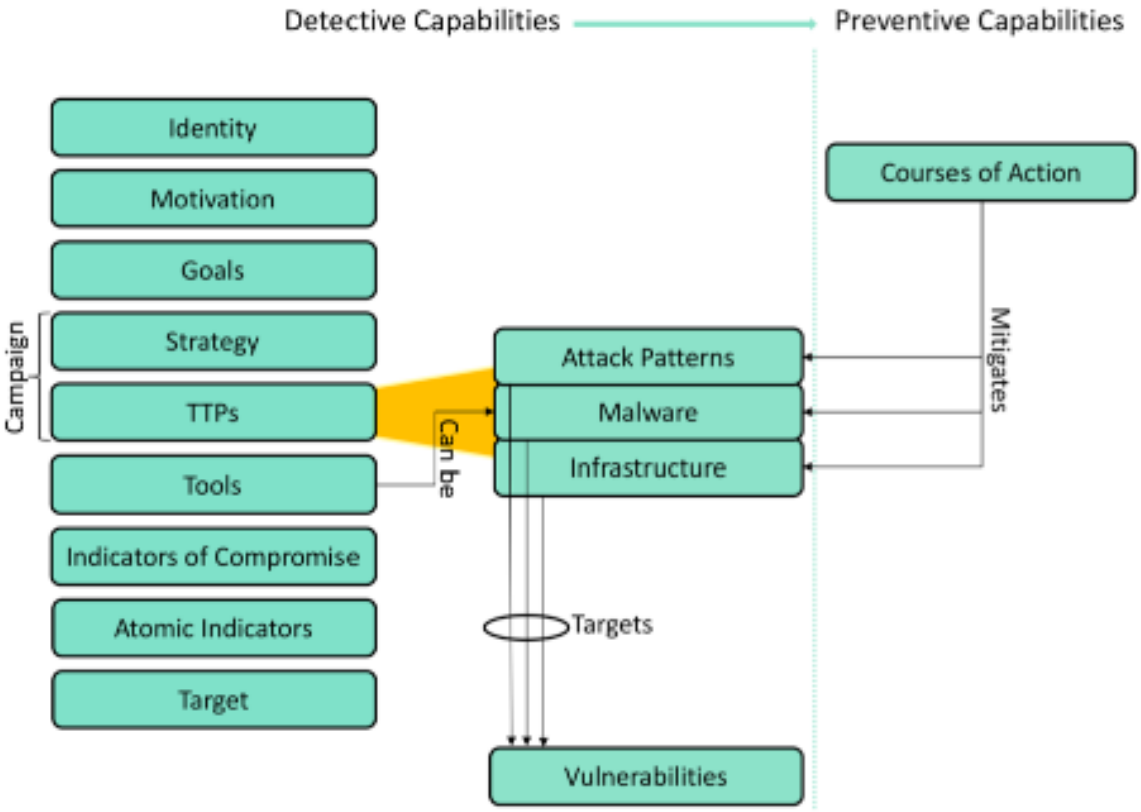
Η Φιλοσοφία του DML μοντέλου μπορούμε να πούμε πως περνάει από τεχνικές παρατηρήσεις σε ανάλυση υψηλού επιπέδου. Το μοντέλο δίνει έμφαση στην ικανότητα ανίχνευσης κυβερνοεπιθέσεων ανάλογα με την ωριμότητα της ομάδας ασφάλειας.

Το μοντέλο δίνει έμφαση στη σύνδεση μεταξύ της ωριμότητας της ανίχνευσης απειλών (Detection Maturity), των πληροφοριών των απειλών (Threat Information) και της ευφυΐας των απειλών (Threat Intelligence). Ωστόσο, υπάρχει μια δυναμική αλληλεπίδραση μεταξύ αυτών των στοιχείων. Ακόμα και ομάδες χαμηλής ικανότητας ανίχνευσης μπορούν να ενισχύσουν την άμυνά τους αξιοποιώντας προηγμένες πληροφορίες απειλών που έχουν παραχθεί από ομάδες με υψηλότερες δυνατότητες ανίχνευσης. Αυτό σημαίνει ότι η ευφυΐα των απειλών μπορεί να αναβαθμιστεί ακόμα και από ώριμες ομάδες χαμηλότερου επιπέδου, καθιστώντας τις πιο ικανές να ανιχνεύουν και να αποτρέπουν κυβερνοεπιθέσεις (Bromander 2017).

2.4.4 The Cyber Threat Intelligence (CTI) Model

Με σκοπό την εξέλιξη, την κοινή χρήση προτύπων και ταξινόμηση των οντολογιών-ταξινομιών, οι Μαυροείδης Βασίλειος και Bromander Siri ανέπτυξαν ένα νέο μοντέλο στο CTI.

Το CTI model είναι ένα ιεραρχικό μοντέλο όπως το DML model που κάναμε αναφορά προηγουμένως αλλά το συγκεκριμένο μοντέλο εστιάζει κυρίως στον τρόπο αναπαράστασης των πληροφοριών που χρειάζονται για πιο εξειδικευμένες κυβερνοαπειλές από μία επίθεση. Η χρήση του συγκεκριμένου μοντέλου από τις ομάδες ασφαλείας των οργανισμών λόγο των προηγμένων ικανοτήτων σε ανίχνευση και πρόληψη μίας επίθεσης το καθιστά ένα «όπλο» στην ασφάλεια του οργανισμού (Bromander 2017).



Εικόνα 7 - Cyber Threat Intelligence Model (Bromander 2017).

Αναλύοντας τους τομείς του μοντέλου:

Ταυτότητα (Identity): Η ταυτότητα ενός επιτιθέμενου (threat actor) μπορεί να είναι η ονομασία του, η ονομασία μιας οργάνωσης ή ακόμη και ενός κράτους. Σε πολλές περιπτώσεις όμως, η ταυτότητα του επιτιθέμενου μπορεί να μην την καθιστά άμεσα αναγνωρίσιμη ή να μην μπορεί με βεβαιότητα να εντοπιστεί ή να προσδιοριστεί σε κάποια συγκεκριμένη τοποθεσία ή οντότητα. Παρόλα αυτά, είναι κρίσιμη η σύνδεση παρόμοιων επιθέσεων στον ίδιο «θύτη», καθώς αυτό βοηθάει στην αναγνώριση των στρατηγικών, των τακτικών, των τεχνικών και των διαδικασιών (TTPs) που χρησιμοποιεί (Bromander 2017).

Κίνητρο (Motivation): Το κίνητρο αναφέρεται σε αυτό που οδηγεί έναν επιτιθέμενο να πραγματοποιήσει μια ενέργεια είτε κακόβουλη είτε όχι, με σκοπό την επίτευξη συγκεκριμένων στόχων προσωπικών ή μη. Συνήθως, το κίνητρο σχετίζεται με τα οφέλη που αποκομίζει ο επιτιθέμενος από την επίτευξη των στόχων που έχει θέσει. Ενώ οι στόχοι ενός επιτιθέμενου μπορεί να αλλάζουν, το κίνητρό του συνήθως παραμένει το ίδιο (Bromander 2017).

Η κατανόηση αυτών των κινήτρων βοηθά:

- Στον προσδιορισμό πιθανών στόχων που μπορεί να επιλέξει.
- Στην εστίαση των αμυντικών πόρων σε πιο πιθανές απειλές.
- Στην πρόβλεψη της έντασης και της επιμονής μιας επίθεσης.

Παραδείγματα τέτοιων κινήτρων μπορεί να είναι:

- Για λόγους ιδεολογίας (π.χ. ανθρώπινα δικαιώματα, εθνικά θέματα)
- Στρατιωτικά συμφέροντα, οικονομικά οφέλη και άλλα.

Στόχοι (Goals): Ο στόχος περιλαμβάνει το τελικό αποτέλεσμα που επιδιώκεται, καθώς και τα μέσα και τις ενέργειες που απαιτούνται για την επίτευξή του. Ο καθορισμός ενός στόχου οδηγεί τη στρατηγική που θα ακολουθήσει ένας επιτιθέμενος. Ανάλογα με τη δομή μιας επίθεσης, οι επιτιθέμενοι μπορεί να μην γνωρίζουν τον τελικό στόχο, αλλά ακολουθούν μια στρατηγική (Bromander 2017).
Στον χώρο του Cyber Threat Intelligence, οι στόχοι συνήθως περιγράφονται με φυσική γλώσσα, όπως:

- Κλοπή πνευματικής ιδιοκτησίας.
- Καταστροφή υποδομών.
- Δυσφήμηση ανταγωνιστή.

Στρατηγική (Strategy): Η στρατηγική είναι η τεχνική περιγραφή του τρόπου με τον οποίο μπορεί να επιτευχθεί μια κυβερνοεπίθεση. Υπάρχουν πολλοί τρόποι για την επίτευξη ενός στόχου, και η στρατηγική καθορίζει ποια κατεύθυνση θα ακολουθήσει ο επιτιθέμενος. Στον τομέα του Cyber Threat Intelligence, οι στρατηγικές περιγράφονται συχνά στη φυσική γλώσσα, γεγονός που δυσκολεύει την ανάλυσή τους. Μια βελτίωση θα ήταν η ανάπτυξη μιας κοινής ταξινομίας, που θα συνδέει τα κίνητρα, τους στόχους και τις στρατηγικές των επιτιθέμενων. Αυτό θα βελτίωνε τη διαχείριση κινδύνων (risk assessment) και την ανάλυση των απειλών (Bromander 2017).
Τακτικές, Τεχνικές και Διαδικασίες (TTPs): Οι τακτικές, τεχνικές και διαδικασίες περιγράφουν τη συμπεριφορά των επιτιθέμενων με βάση:

- Τι κάνουν (Tactics).
- Πώς το κάνουν (Techniques).
- Ποια ακριβώς τα βήματα που ακολουθούν (Procedures).

Τα TTPs περιλαμβάνουν διάφορες κατηγορίες, όπως:

- Μοτίβα επιθέσεων (Attack Patterns): Περιγράφουν συγκεκριμένους τρόπους που χρησιμοποιούν οι επιτιθέμενοι για να παραβιάσουν έναν στόχο.
- Κακόβουλο λογισμικό (Malware): Πρόγραμμα που εισάγεται σε ένα υπολογιστικό σύστημα με σκοπό την παραβίαση της εμπιστευτικότητας, της ακεραιότητας ή της διαθεσιμότητας.
- Υποδομή (Infrastructure): Οι πόροι που διαθέτουν οι επιτιθέμενοι για να εκτελέσουν επιθέσεις (Bromander 2017).

Εργαλεία (Tools): Οι επιτιθέμενοι αν καταφέρουν και εισέλθουν στο σύστημα-δίκτυο του στόχου-θύματος, εγκαθιστούν και χρησιμοποιούν εργαλεία τα οποία συχνά τροποποιούνται έτσι ώστε να αποφεύγεται η ανίχνευση τους. Το malware είναι μια υποκατηγορία εργαλείων, αλλά υπάρχουν και εργαλεία που δεν είναι απαραίτητα κακόβουλα αλλά χρησιμοποιούνται κακόβουλα (Bromander 2017).
Indicators of Compromise (IOCs): Είναι στοιχεία που βοηθούν στην ανίχνευση κακόβουλων δραστηριοτήτων και στην ταυτοποίηση συγκεκριμένων μοτίβων επιθέσεων, TTPs, κακόβουλου λογισμικού, εργαλείων και κακόβουλων οντοτήτων. Για τη δημιουργία αξιόπιστων IOCs, είναι χρήσιμο να συνδυάζονται διαφορετικοί τύποι πληροφοριών, όπως:

- Atomic Indicators (IPs, domain names, file hashes).
- Behavioral Indicators (ανωμαλίες σε μοτίβα).
- Computed Indicators (συσχετίσεις δεδομένων από πολλαπλές πηγές).

Atomic Indicators: Είναι βασικά στοιχεία αναγνώρισης απειλών, όπως IP διευθύνσεις, ονόματα παρόχων, hashes αρχείων, κ.λπ. Παρόλο που χρησιμοποιούνται εκτενώς στο Cyber Threat Intelligence, έχουν μικρή διάρκεια ζωής, καθώς οι επιτιθέμενοι μπορούν εύκολα να τα αλλάξουν (Bromander 2017).

Στόχοι (Targets): Οι στόχοι των κυβερνοεπιθέσεων μπορεί να είναι:

- Οργανισμοί και επιχειρήσεις.
- Διάφοροι κλάδοι στη βιομηχανία.
- Κυβερνήσεις και κρατικές υπηρεσίες.
- Στρατιωτικές εγκαταστάσεις.
- Μεμονωμένα άτομα.

Σχέδια Δράσης (Courses of Action - CoA): Τα Σχέδια Δράσης περιλαμβάνουν τα μέτρα που μπορούν να ληφθούν για την πρόληψη ή την αντιμετώπιση ενάντια σε κυβερνοεπιθέσεις (Bromander 2017)

Κεφάλαιο 3ο: SKOS (Simple Knowledge Organization System)

3.1 Τι είναι το SKOS;

Το Simple Knowledge Organization System (SKOS) είναι ένα πρότυπο που αναπτύχθηκε από το W3C για την αναπαράσταση και την καλύτερη διαχείριση όρων-εννοιών, λεξιλογίων, ταξινομιών, θησαυρών στο διαδίκτυο. Το SKOS βασίζεται στην τεχνολογία του Σημασιολογικού Ιστού, αξιοποιώντας το RDF (Recourse Description Framework) για την καλά δομημένη αναπαράσταση της γνώσης-πληροφορίας. Η κυριότερη λειτουργία του SKOS είναι η καλή οργάνωση των εννοιών-όρων μέσω ενός απλού και ευέλικτου μοντέλου που μπορεί να χρησιμοποιηθεί σε πολλούς και διαφορετικούς τομείς. Αντί να απαιτεί πολύπλοκα σχήματα οντολογιών όπως αυτών του μοντέλου OWL, το SKOS παρέχει έναν πιο φιλικό και πιο κατανοητό τρόπο για την αναπαράσταση της γνώσης-πληροφορίας, έχοντας έτσι διαλειτουργικότητα στην ανταλλαγή της γνώσης και των δεδομένων μεταξύ διαφορετικών συστημάτων (W3C 1994-2012).
Το μοντέλο χρησιμοποιείται ευρέως από τις κυβερνήσεις (π.χ. Δημόσιος Τομέας του Ηνωμένου Βασιλείου, Λεξιλόγια, Θεματικές Επικεφαλίδες Γαλλικής Εθνικής Βιβλιοθήκης, Θεματικές επικεφαλίδες της Βιβλιοθήκης του Κογκρέσου των Ηνωμένων Πολιτειών), από επιστημονικούς φορείς (π.χ. Διεθνές Εικονικό Παρατηρητήριο Alliance Astronomy Vocabulary, λεξιλόγια NASA, Thesaurus για τις Κοινωνικές Επιστήμες) και μη κυβερνητικές οργανισμοί (π.χ. Wikipedia, UNESCO Thesaurus, Γενικός Πολύγλωσσος Περιβαλλοντικός Θησαυρός). Σε αντίθεση με την κοινοπραξία World Wide Web πρότυπο σημασιολογικού Ιστού και την Γλώσσα Οντολογίας Ιστού (OWL), η SKOS ακολουθεί την αρχή της «ελάχιστης δέσμευσης οντολογίας». SKOS έννοιες και οι σχέσεις προσδιορίζονται χρησιμοποιώντας «ευρύτερες» σχέσεις τύπου θησαυρού παρά λογικά επισημοποιημένες σχέσεις που χρησιμοποιείται συνήθως στην OWL (Mike Conway 2016).

3.2 Κύρια χαρακτηριστικά του SKOS

Τα SKOS δεδομένα εκφράζονται ως τριπλέτες RDF. Αυτό σημαίνει ότι οι έννοιες μπορούν να λειτουργούν είτε ως υποκείμενα είτε ως αντικείμενα, συνδεδεμένα μέσω μιας ιδιότητας SKOS, η οποία παίζει τον ρόλο του πρόσημου (predicate). Κάθε έννοια στο SKOS μπορεί να αναγνωριστεί μέσω URI (Uniform Resource Identifier) με μοναδικό τρόπο. Τα URI μπορούν να οριστούν με συστήματα μόνιμων αναγνωριστικών. Αν και το SKOS δεν επιβάλλει τη χρήση μόνιμων αναγνωριστικών, είναι ιδιαίτερα συνιστώμενη στο πλαίσιο των Διασυνδεδεμένων Ανοικτών Δεδομένων (Linked Open Data) (Holland 2010).

Το SKOS περιλαμβάνει διάφορες κλάσεις για την οργάνωση και την αναπαράσταση της πληροφορίας ή γνώσης. Παρακάτω αναφέρονται και αναλύονται οι κύριες κλάσεις του μοντέλου, καθώς και οι σχέσεις τους και η χρησιμότητα της κάθε μίας. Στο κεφάλαιο 3.2 που εξετάζουμε όλες οι πληροφορίες αντλήθηκαν από (Bechhofer 2008).

3.2.1 skos:Consept

URI: http://www.w3.org/2008/05/skos#Concept
Ορισμός: Το skos:Concept είναι η βασική κλάση στο SKOS και αντιπροσωπεύει μια αφηρημένη έννοια.
Χρησιμοποιείται για την αναπαράσταση εννοιών σε ταξινομίες, θησαυρούς, λεξιλόγια και άλλα σχήματα. Κάθε έννοια έχει:

- skos:prefLabel Προτιμώμενη ετικέτα.
- skos:altLabel Εναλλακτικές ετικέτες.
- skos:note Σημειώσεις Τεκμηρίωσης.
- skos:definition Σημειώσεις Τεκμηρίωσης.
- skos:scopeNote Σημειώσεις Τεκμηρίωσης.

Σχέσεις:
Είναι ασυμβίβαστο (Disjoint) με κλάσεις:

- skos:Collection Δεν μπορεί να είναι ταυτόχρονα συλλογή και έννοια.
- skos:ConseptScheme Δεν μπορεί να είναι ταυτόχρονα έννοια και ένα σχήμα εννοιών.

3.2.2 skos:ConseptSheme

URI: http://www.w3.org/2008/05/skos#ConceptScheme
Ορισμός: Η skos:ConceptScheme κλάση χρησιμοποιείται για να οργανώσει και να ομαδοποιήσει σύνολα εννοιών που ανήκουν στο ίδιο σύστημα γνώσης (π.χ., ένα θησαυρό, μια ταξινομία ή ένα λεξιλόγιο).
Ένα ConceptScheme μπορεί να περιλαμβάνει πολλές έννοιες skos:Concept. Μπορεί να αντιστοιχεί σε ένα θησαυρό όρων, ένα σύστημα ταξινόμησης ή μια άλλη οντολογία. Συνήθως χρησιμοποιείται με τις ιδιότητες:

- skos:hasTopConsept Δηλώνει τις κύριες έννοιες ενός σχήματος.
- skos:inScheme Συσχετίζει τις έννοιες με ένα συγκεκριμένο σχήμα.
- skos:prefLabel Για την τεκμηρίωση του σχήματος.
- skos:definition Για την τεκμηρίωση του σχήματος.
- skos:note Για την τεκμηρίωση του σχήματος.

Σχέσεις:
Είναι ασυμβίβαστο (Disjoint) με κλάσεις:

- skos:Collection Δεν μπορεί να είναι ταυτόχρονα και συλλογή.
- skos:ConseptScheme Το σχήμα δεν είναι έννοια, αλλά τις οργανώνει.

3.2.3 skos:Collection

URI: http://www.w3.org/2008/05/skos#Collection
Ορισμός: Η skos:Collection κλάση ομαδοποιεί το συνόλων των εννοιών χωρίς να δημιουργείται μία αυστηρή ιεραρχία.
Μια κλάση Collection περιλαμβάνει έννοιες μέσω της ιδιότητας skos:member και δεν δημιουργεί ιεραρχικές σχέσεις (όπως η skos:broader και η skos:narrower). Είναι χρήσιμη σε περιπτώσεις όπου οι έννοιες απλά σχετίζονται στο ίδιο θέμα ή χρησιμοποιούνται μαζί σε συγκεκριμένα σχήματα.
Σχέσεις:
Είναι ασυμβίβαστο (Disjoint) με κλάσεις:

- skos:Consept Δεν μπορεί να είναι ταυτόχρονα έννοια και συλλογή.
- skos:ConseptScheme Το σχήμα δεν είναι έννοια, αλλά τις οργανώνει.

3.2.4 skos:OrderedCollection

URI: http://www.w3.org/2008/05/skos#OrderedCollection
Ορισμός: Η skos:OrderedCollection κλάση είναι μια ειδική εκδοχή της skos:Collection, όπου η σειρά των εννοιών είναι σημαντική.

Διαφέρει από την skos:Collection γιατί χρησιμοποιεί την ιδιότητα skos:memberList για να ορίσει σειρά στα μέλη της. Είναι χρήσιμη σε διαδικασίες που πρέπει να ακολουθείται μία σειρά και σε συστήματα εννοιών εκπαίδευσης, όπου εκεί οι έννοιες έχουν συγκεκριμένη αλληλουχία.
Σχέσεις:

- Δεν είναι ασυμβίβαστες με άλλες κλάσεις, χρησιμοποιείται όμως σε ειδικές περιπτώσεις.
- Είναι υπερκλάση της skos:Collection.

Συγκεντρωτικά με τα παραπάνω μπορούμε να δώσουμε τον εξής πίνακα κλάσεων:

Πίνακας 1 - Ανάλυση κύριων κλάσεων SKOS

Κλάση	Περιγραφή	Βασικές Ιδιότητες	Disjoint με
Skos:Consept	Αντιπροσωπεύει μια έννοια.	skos:prefLabel, skos:broader, skos:narrower, skos:related	skos:Collection, skos:ConceptScheme
Skos:ConseptScheme	Σχήμα που οργανώνει έννοιες.	skos:hasTopConcept, skos:inScheme	skos:Collection, skos:Concept
Skos:Collection	Ομαδοποίηση εννοιών (μη ιεραρχική).	skos:member	skos:Concept, skos:ConceptScheme
Skos:OrderedCollection	Ομαδοποίηση εννοιών με συγκεκριμένη σειρά.	skos:memberList	-

Το SKOS κατέχει ένα σύνολο ιδιοτήτων (properties) που χρησιμοποιούνται για τη διαχείριση, τεκμηρίωση και συσχέτιση των εννοιών. Παρακάτω αναλύονται οι βασικές ιδιότητες του SKOS με βάση τις κύριες κατηγορίες τους.

3.2.5 Ετικέτες

Οι ιδιότητες αυτές χρησιμοποιούνται για να δώσουν λεξική ετικέτα σε έννοιες (cosncepts), διευκολύνοντας την αναζήτηση τους.
skos:prefLabel

- URI**:** http://www.w3.org/2008/05/skos#prefLabel
- *Ορισμός*: Καθορίζει την προτεινόμενη ετικέτα που θα έχει η έννοια σε μία συγκεκριμένη γλώσσα. Κάθε έννοια μπορεί να έχει μόνο μία προτιμώμενη ετικέτα ανά γλώσσα.
- Super property: rdfs:label

skos: altLabel

- URI: http://www.w3.org/2008/05/skos#altLabel
- *Ορισμός*: Καθορίζει ενναλακτική ετικέτα που θα έχει η έννοια σε μία συγκεκριμένη γλώσσα όπως κοινές έννοιες ή συνώνυμες. Κάθε έννοια μπορεί να έχει περισσότερες από μία ενναλακτικές ετικέτες.
- Super property: rdfs:label

skos:hiddenLabel

- URI: http://www.w3.org/2008/05/skos#hiddenLabel
- *Ορισμός*: Καθορίζει **μη ορατές** ετικέτες και χρησιμοποιούνται για σκοπούς αναζήτησης.

3.2.6 Σημασιολογικές Σχέσεις

Αυτές οι ιδιότητες ορίζουν τις σχέσεις μεταξύ εννοιών, επιτρέποντας τη δημιουργία ιεραρχιών και συνδέσεων.

skos:broader

- URI: http://www.w3.org/2008/05/skos#broader
- *Ορισμός*: Δηλώνει ότι μια έννοια έχει μια ευρύτερη σχέση (είναι «γονιός») με μια άλλη έννοια.
- Inverse of: skos:narrower

skos:narrower

- URI**:** http://www.w3.org/2008/05/skos#narrower
- *Ορισμός***:** Δηλώνει ότι μια έννοια έχει μια στενότερη σχέση (είναι «παιδί») με μια άλλη έννοια.
- Inverse of: skos:broader

skos:related

- URI: http://www.w3.org/2008/05/skos#related
- *Ορισμός*: Δηλώνει ότι δύο έννοιες σχετίζονται μεταξύ τους στο ίδιο σχήμα αλλά δεν έχουν ιεραρχική σχέση μεταξύ τους.
- Χαρακτηριστικό**:** Συμμετρική (Symmetric)

skos:broaderTransitive

- URI: http://www.w3.org/2008/05/skos#broaderTransitive
- *Ορισμός*: Δηλώνει μια ευρύτερη σχέση μετάβασης, επιτρέποντας την αναζήτηση ιεραρχιών σε επίπεδα.

skos:narrowerTransitive

- URI: http://www.w3.org/2008/05/skos#narrowerTransitive
- *Ορισμός*: Δηλώνει μια στενή σχέση μετάβασης και την σύνδεση εννοιών πολλαπλών επιπέδων.

3.2.7 Χαρτογράφηση Σχέσεων

Αυτές οι ιδιότητες χρησιμοποιούνται για τη σύνδεση εννοιών μεταξύ διαφορετικών λεξιλογίων ή ταξινομιών ή σχημάτων.

skos:closeMatch

- URI: http://www.w3.org/2008/05/skos#closeMatch
- *Ορισμός*: Δηλώνει ότι δύο έννοιες είναι αρκετά παρόμοιες μεταξύ τους αλλά όχι και ταυτόσημες.
- Χαρακτηριστικό: Συμμετρική (Symmetric)

skos:exactMatch

- URI: http://www.w3.org/2008/05/skos#exactMatch
- *Ορισμός*: Δηλώνει ότι δύο έννοιες είναι ταυτόσημες και μπορούν να χρησιμοποιηθούν εναλλακτικά μεταξύ διαφορετικών λεξιλογίων ή ταξινομιών ή σχημάτων.
- Χαρακτηριστικά: Συμμετρική και Μεταβατική (Symmetric, Transitive)

skos:broadMatch

- URI: http://www.w3.org/2008/05/skos#broadMatch
- *Ορισμός*: Δηλώνει μια ευρύτερη αντιστοίχιση μεταξύ δύο εννοιών από διαφορετικά λεξιλόγια.
- Super property: skos:broader

skos:narrowMatch

- URI: http://www.w3.org/2008/05/skos#narrowMatch
- *Ορισμός*: Δηλώνει μια στενή αντιστοίχιση μεταξύ δύο εννοιών από διαφορετικά λεξιλόγια.
- Inverse of: skos:broadMatch

3.2.8 Ιδιότητες Τεκμηρίωσης

Αυτές οι ιδιότητες παρέχουν την τεκμηρίωση καθώς και επιπλέον πληροφορίες για μια έννοια.

skos:definition

- *Ορισμός*: Μας δίνει έναν ορισμό για μία έννοια.
- Super property: skos:note

skos:scopeNote

- *Ορισμός*: Διευκρινίζει το πεδίο εφαρμογής της έννοιας ή τη χρήση της.

skos:editorialNote

- *Ορισμός*: Χρησιμοποιείται για σημειώσεις ή σχόλια των διαχειριστών της ταξινομίας.

skos:changeNote

- *Ορισμός*: Αναφέρεται σε τροποποιήσεις και αλλαγές που έγιναν στην έννοια του σχήματος.

skos:example

- *Ορισμός*: Μας δίνει παραδείγματα που βοηθούν στην κατανόηση της αναφερόμενης έννοιας.

3.2.9 Ιδιότητες Συλλογών

Οι ιδιότητες αυτές χρησιμοποιούνται για τη διαχείριση συλλογών από έννοιες.

skos:member

Ορισμός: Συνδέει μια συλλογή με τις έννοιες που περιλαμβάνει.

skos:memberList

Ορισμός: Χρησιμοποιείται για να ορίσει μία συγκεκριμένη σειρά από τα συμπεριλαμβανόμενα μέλη μιας OrderedCollection.
Συγκεντρωτικά με τα παραπάνω μπορούμε να δώσουμε τον εξής πίνακα ιδιοτήτων που παρέχει μια συνοπτική αλλά πλήρη περιγραφή των βασικών ιδιοτήτων του **SKOS**, οι οποίες χρησιμοποιούνται για τη διαχείριση ταξινομιών, θησαυρών και συστημάτων παροχής πληροφοριών:

Πίνακας 2 - Ανάλυση ιδιοτήτων SKOS

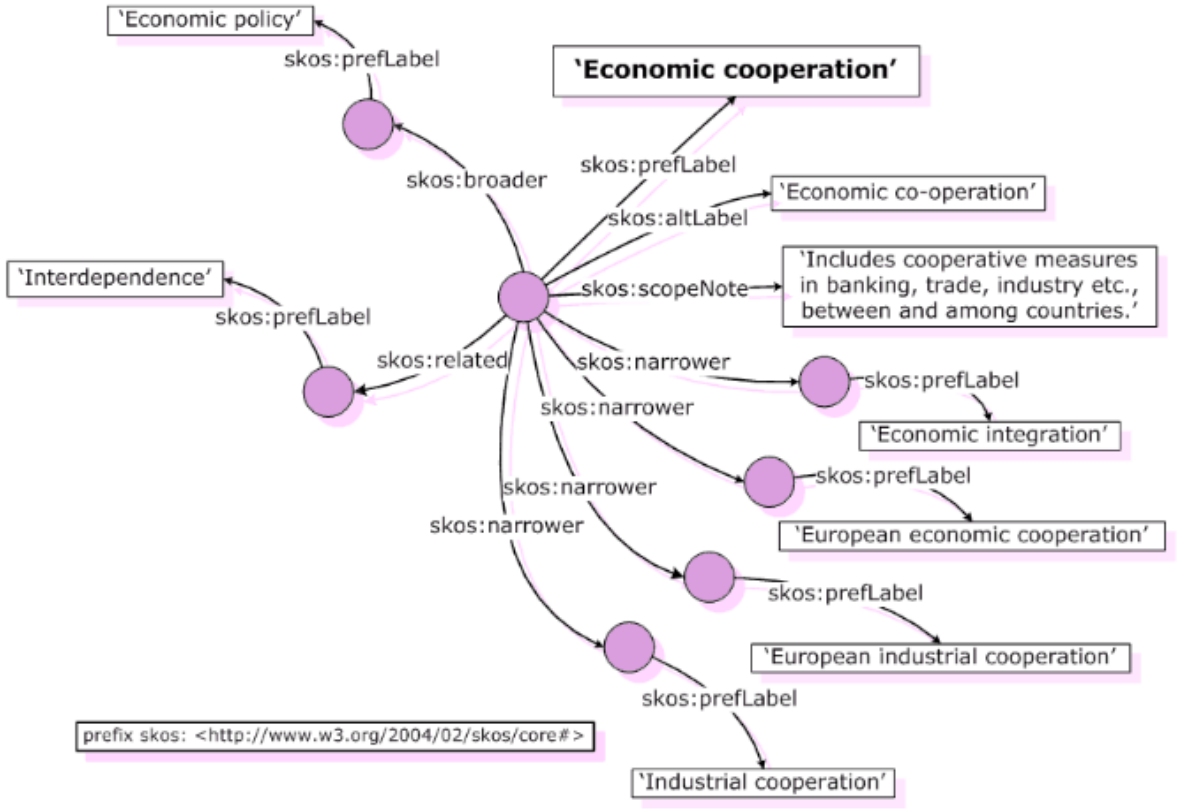
Κατηγορία	Ιδιότητα	Περιγραφή	Χαρακτηριστικά
Ετικέτες	skos:prefLabel	Ορίζει την προτιμώμενη ετικέτα μιας έννοιας.	Μία μόνο προτιμώμενη ετικέτα ανά γλώσσα.
	skos:altLabel	Ορίζει εναλλακτικές ετικέτες (συνώνυμα, ή παραλλαγές).	Μπορεί να έχει πολλές ανά γλώσσα.
	skos:hiddenLabel	Ορίζει ετικέτες μη ορατές που χρησιμοποιούνται στην αναζήτηση.	-
Σημασιολογικές Σχέσεις	skos:broader	Δηλώνει μια ευρύτερη έννοια.	Inverse of skos:narrower.
	skos:narrower	Δηλώνει μια στενή έννοια.	Inverse of skos:broader.
	skos:related	Δηλώνει μια σχέση μεταξύ 2 εννοιών.	Συμμετρική σχέση.
	skos:broaderTransitive	Ευρύτερη σχέση που επιτρέπει την μετάβαση.	Μεταβατική σχέση.
	skos:narrowerTransitive	Στενή σχέση που επιτρέπει την μετάβαση.	Μεταβατική σχέση.
Χαρτογράφηση Σχέσεων	skos:closeMatch	Δηλώνει ότι δύο έννοιες είναι αρκετά παρόμοιες.	Συμμετρική σχέση.

	skos:exactMatch	Δηλώνει ότι δύο έννοιες είναι ταυτόσημες.	Συμμετρική & μεταβατική σχέση.
	skos:broadMatch	Δηλώνει μια ευρύτερη αντιστοίχιση μεταξύ λεξιλογίων.	Super property: skos:broader.
	skos:narrowMatch	Δηλώνει μια στενή αντιστοίχιση μεταξύ λεξιλογίων.	Inverse of skos:broadMatch.
Ιδιότητες Τεκμηρίωσης	skos:definition	Ορισμός της έννοιας.	-
	skos:scopeNote	Διευκρινίζει το πεδίο εφαρμογής μιας έννοιας.	-
	skos:editorialNote	Χρησιμοποιείται για σχόλια επεξεργασίας.	-
	skos:changeNote	Αναφέρει αλλαγές και ενημερώσεις μιας έννοιας.	-
	skos:example	Παρέχει παραδείγματα για μια έννοια.	-
Ιδιότητες Συλλογών	skos:member	Συνδέει μια συλλογή με τις έννοιες που περιλαμβάνει.	Χρησιμοποιείται για skos:Collection.
	skos:memberList	Ορίζει τη σειρά των μελών μιας συλλογής.	Χρησιμοποιείται για skos:OrderedCollection.

3.2.10 Χρήση του SKOS στην Αναπαράσταση Εννοιών

Στην παρακάτω εικόνα παρουσιάζεται ένα παράδειγμα εφαρμογής του SKOS για την οργάνωση εννοιών. Είναι ένα απόσπασμα από τον θησαυρό UK Archival Thesaurus (UKAT), στο οποίο αναπαρίσταται η έννοια "Economic cooperation με τις σχέσεις που έχει με άλλες έννοιες.

Εδώ αποδίδονται οι σχέσεις αυτές σε μορφή RDF Graph:



Εικόνα 8 - Γράφημα RDF με λεξικό SKOS Core (Brickley 2005)

Το διάγραμμα RDF που χρησιμοποιεί το SKOS Core Vocabulary δείχνει τις διάφορες σημασιολογικές σχέσεις μεταξύ των εννοιών, όπως οι: skos:broader: Ορίζει μια ευρύτερη έννοια (σχέσεις γονεα-παιδιού), π.χ., η "Economic policy" είναι η γενική έννοια της "Economic cooperation". skos:narrower: Ορίζει πιο εξειδικευμένες έννοιες (σχέσεις γονεα-παιδιού), π.χ., "European economic cooperation" και "Industrial cooperation". skos:related: Δηλώνει ότι δύο έννοιες σχετίζονται θεματικά, όπως η "Interdependence" με την "Economic cooperation". skos:prefLabel: Δείχνει την προτιμώμενη ετικέτα κάθε έννοιας. skos:scopeNote: Περιέχει πρόσθετες πληροφορίες για την χρήση της έννοιας (Brickley 2005).

3.3 Σύγκριση SKOS με άλλα μοντέλα

Το SKOS είναι ένα μοντέλο για την αναπαράσταση λεξικών όρων, όπως θησαυροί, ταξινομίες και συστήματα κατηγοριοποίησης της γνώσης όπως είναι οι οντολογίες. Ωστόσο, υπάρχουν άλλα μοντέλα που χρησιμοποιούνται για παρόμοιους ή και πιο εξειδικευμένους σκοπούς, όπως το OWL και το STIX. Το SKOS και το OWL είναι δύο πρότυπα του W3C που χρησιμοποιούνται για την αναπαράσταση γνώσης, αλλά εξυπηρετούν διαφορετικούς σκοπούς και έχουν διαφορετική πολυπλοκότητα.

3.3.1 Σύγκριση SKOS με OWL

Το OWL είναι μια γλώσσα που επιτρέπει την αναπαράσταση σύνθετων οντολογιών με αυστηρή ιεραρχία. Υποστηρίζει κλάσεις, ιδιότητες, σχέσεις, επιτρέποντας την αυτόματη εξαγωγή συμπερασμάτων μέσω μηχανισμών λογικής (W3C 2012).
Παρακάτω μπορούμε να δώσουμε τον πίνακα σύγκρισης μεταξύ των SKOS και OWL:

Πίνακας 3 - Σύγκριση SKOS με OWL

	SKOS	OWL
ΣΚΟΠΟΣ	Οργάνωση όρων, θησαυρών και ταξινομιών	Έκφραση πολύπλοκων σημασιολογικών σχέσεων
ΤΥΠΟΣ	Λεξιλόγιο (thesaurus, taxonomy)	Οντολογίες με αυστηρές σημασιολογικές σχέσεις
ΙΕΡΑΡΧΙΑ	Περιορισμένη, εστιάζει σε απλές σημασιολογικές σχέσεις	Πιο εξελιγμένη ιεραρχία μέσω owl:Class και rdfs:subClassOf
ΠΕΡΙΟΡΙΣΜΟΙ	Εστιάζει σε απλές σημασιολογικές σχέσεις	Έχει περιορισμούς (cardinality, domain, range)
ΠΟΤΕ ΝΑ ΧΡΗΣΙΜΟΠΟΙΗΘΕΙ	Όταν χρειάζεται απλή δομή ταξινόμησης.	Όταν απαιτούνται περίπλοκες λογικές σχέσεις μεταξύ οντοτήτων

3.3.2 Σύγκριση SKOS με STIX

Το STIX είναι ένα πρότυπο σχεδιασμένο για την αναπαράσταση και ανταλλαγή πληροφοριών σχετικά με απειλές στον κυβερνοχώρο. Περιλαμβάνει λεπτομερής έννοιες για την περιγραφή απειλών, τακτικών, τεχνικών και διαδικασιών που χρησιμοποιούνται από επιτιθέμενους (Open 2017-2024).

Παρακάτω μπορούμε να δώσουμε τον πίνακα σύγκρισης μεταξύ των SKOS και OWL:

Πίνακας 4 - Σύγκριση SKOS με STIX

	SKOS	STIX
ΣΚΟΠΟΣ	Οργάνωση όρων, θησαυρών και ταξινομιών	Μοντελοποίηση πληροφοριών για κυβερνοαπειλές
ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ	Βιβλιοθήκες, μουσεία, ταξονομίες δεδομένων	Cyber Threat Intelligence (CTI), κυβερνοασφάλεια
ΤΥΠΟΣ ΔΕΔΟΜΕΝΩΝ	Εννοιολογικές σχέσεις (π.χ. broader/narrower)	Δομημένα αντικείμενα για απειλές (Indicators, TTPs, Observables)
ΧΡΗΣΗ ΣΕ CTI	Βοηθά στη δημιουργία οντολογίας κυβερνοαπειλών	Πρότυπο για την ανταλλαγή πληροφοριών απειλών

3.3.3 Σύγκριση SKOS με Θησαυρούς

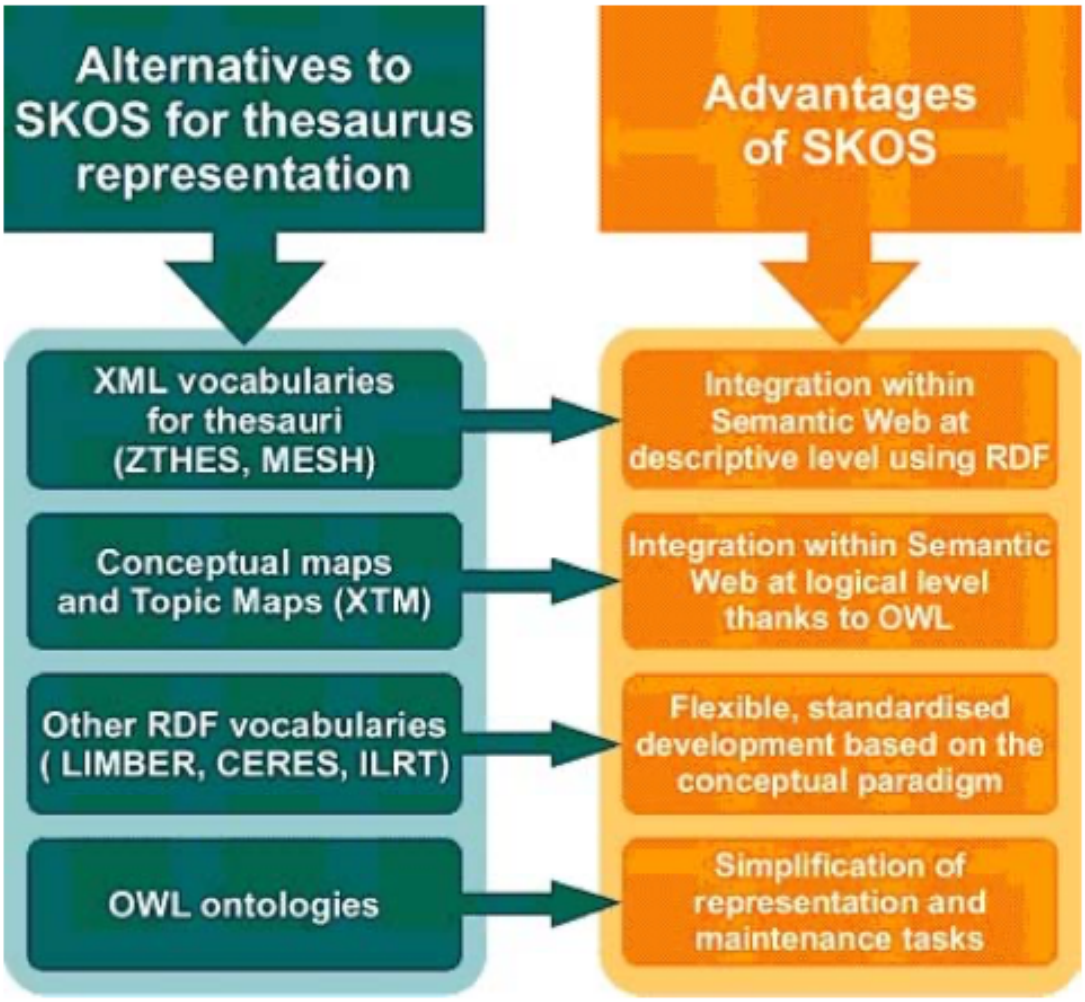
Η SKOS προσφέρει μια πιο στενή προσέγγιση στην οργάνωση και διαχείριση της γνώσης, συμπληρώνοντας την αυτόματη εξαγωγή κειμένου από έγγραφα με ευρετηρίασή του μέσω εννοιολογικών οντοτήτων. Οι θησαυροί μπορούν να συνδυαστούν με αμοιβαίο τρόπο μέσω εξαρτημένων σχέσεων, επιτρέποντας την επαναχρησιμοποίησή τους και την πιο

αποτελεσματική χρήση της ευρετηρίασης και της κατασκευής συστημάτων αναζήτησης πληροφοριών Ιστού. Το SKOS επιτρέπει εργαλεία αναζήτησης πολλαπλών επιπέδων και αυτό μας δίνει ένα μοντέλο δομημένο με διαφορετικά επίπεδα: εννοιολογικά, αναζήτησης και τεκμηρίωσης. Οι θησαυροί οργανώνουν τις έννοιες σε επίπεδα, μία λύση στην διαδικασία ανάκτησης των πληροφοριών με δυνατότητα αναζήτησης από υπερ-συνδέσμους σε ιστοσελίδες. Οι θησαυροί θα μπορούσαν να επαναπροσδιορίσουν την επέκταση των αναζητήσεων με την εμφάνιση εγγράφων με σχετικό περιεχόμενο με αυτό που αναζητήθηκε κθώς και με την αναζήτηση με λέξεις-κλειδιά σε ένα πλαίσιο εννοιών επιλέγοντας την κατάλληλη προς αναζήτηση έννοια (Juan-Antonio Pastor-Sanchez 2009).
Παρακάτω μπορούμε να δώσουμε τον πίνακα σύγκρισης μεταξύ των SKOS και Thesaurus:

Πίνακας 5 - Σύγκριση SKOS με THESAURUS

	SKOS	**THESAURUS**
ΣΚΟΠΟΣ	Ψηφιακή αναπαράσταση εννοιών με δομή Σημασιολογικού Ιστού	Οργάνωση και διαχείριση ελεγχόμενων λεξιλογίων
ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ	Semantic Web, πληροφοριακά συστήματα, ψηφιακές βιβλιοθήκες	Βιβλιοθήκες, αρχεία, μουσεία, συστήματα τεκμηρίωσης
ΔΟΜΗ	RDF-based, συνδέει έννοιες με: skos:broader, skos:narower, skos:related	Ιεραρχική δομή με κανόνες όπως ISO 25964 και ANSI/NISO Z39.19
ΔΙΑΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ	Υποστηρίζει Linked Data και τη χαρτογράφηση εννοιών με: skos:exactMatch, skos:closeMatch	Περιορισμένη διαλειτουργικότητα, συχνά απαιτεί μετατροπή δεδομένων
ΕΥΕΛΙΞΙΑ	Εύκολο στην υιοθέτηση και προσαρμογή σε διαφορετικά συστήματα	Αυστηροί κανόνες για τη δημιουργία και διαχείριση σχέσεων
ΕΠΕΚΤΑΣΙΜΟΤΗΤΑ	Μπορεί να ενσωματωθεί με OWL και άλλες οντολογίες	Περιορισμένη δυνατότητα επέκτασης

Παρακάτω μπορούμε να δούμε και ενναλακτικά μοντέλα σύνταξης θησαυρών με τα πλεονεκτήματα του μοντέλου SKOS:



Εικόνα 9 - Πλεονεκτήματα του SKOS σε σχέση με άλλες ενναλακτικές δημιουργίας θησαυρών (Juan-Antonio Pastor-Sanchez 2009)

Συμπερασματικά με την σύγκριση των μοντέλων που αναφέρθηκαν μπορούμε να επισυμάνουμε πως:

- Η χρήση SKOS είναι κατάλληλη για την αναπαράσταση απλών ιεραρχιών ή σχέσεων μεταξύ εννοιών, όπως σε θησαυρούς ή ταξινομίες, χωρίς μεγάλη πολυπλοκότητα και δεν απαιτούνται αυστηροί περιορισμοί.
- Η χρήση OWL προτιμάται στην αναπαράσταση σύνθετων και αυστηρών δομών γνώσης, όπως όταν απαιτείται η αυτόματη εξαγωγή συμπερασμάτων ή η επαλήθευση των δεδομένων.
- Το STIX προσφέρει μια εξειδικευμένη αναπαράσταση των απειλών, καθιστώντας το πιο κατάλληλο για την εφαρμογή του στον τομέα της κυβερνοασφάλειας.

3.4 Πρακτική Χρήση του SKOS στο CTI

Λαμβάνοντας υπόψιν όλα τα παραπάνω μπορούμε να απαντήσουμε στο ερώτημα: Πώς μπορεί το μοντέλο SKOS να βοηθήσει στην οργάνωση των εννοιών, πληροφοριών ή όρων κυβερνοαπειλών στον τομέα του Cyber Threat Intelligence.

Το SKOS μπορεί να χρησιμεύσει για τη δημιουργία λεξιλογίων, οντολογιών και θησαυρών που βοηθούν στην κατηγοριοποίηση των όρων στην ανάλυση των κυβερνοαπειλών. Αυτό καθιστά ποιο εύκολη την την ανάκτηση των πληροφοριών, επιτρέποντας στους ειδικούς του cyber security να εντοπίζουν και να αναλύουν τις απειλές με μεγαλύτερη ακρίβεια. Χρσησιμοποιόντας το πλαίσιο του MITRE ATT&CK, μπορεί να δημιουργιθεί μια δομημένη ταξονομία που μπορεί να ενσωματωθεί σε ένα συστήματα CTI. Επιπλέον, συμπληρωματικά με το STIX 2.0, μπορεί να παρέχει μια απλή και ευανάγνωστη αναπαράσταση, ενώ με το STIX 2.0 προσφέρει μια πιο λεπτομερή και αυστηρή δομή για την ανταλλαγή των πληροφοριών των απειλών.

Στο επόμενο κεφάλαιο θα παρουσιάσουμε και θα εξετάσουμε βήμα βήμα, τη διαδικασία δημιουργίας μιας οντολογίας βασισμένης στο μοντέλο SKOS, με στόχο την οργάνωση και διαχείριση των όρων-πληροφοριών στον τομέα του Cyber Threat Intelligence. Θα δούμε πώς μπορούμε να χρησιμοποιήσουμε το SKOS για την αναπαράσταση αυτών των εννοιών, όπως τύποι απειλών, τακτικές που χρησιμοποιούνται, δείκτες παραβίασης (IoCs) και πολλά άλλα, δημιουργώντας μια καλά δομημένη με αυστηρή ιεραρχία οντολογία. Στην προσέγγιση αυτή, θα αναλύσουμε τις βασικές αρχές της ιεραρχικής δομής, θα κατανοήσουμε πώς οι έννοιες συνδέονται μεταξύ τους και θα δούμε πώς μπορούμε να αξιοποιήσουμε το SKOS για να δημιουργήσουμε ένα εύκολο, εύχρηστο και επεκτάσιμο μοντέλο γνώσης ανάλυσης κυβερνοαπειλών.

Κεφάλαιο 4ο: Μεθοδολογία

Σε αυτό το κεφάλαιο, περιγράφεται όλη η διαδικασία κατά την οποία αναπτύχθηκε η οντολογία Cyber Threat Intelligence χρησιμοποιώντας το μοντέλο SKOS στο Protege. Η μεθοδολογία που ακολουθήθηκε έχει ως βάση μια δομημένη και περιοδική διαδικασία που περιλαμβάνει τη συλλογή και ανάλυση δεδομένων, τη μοντελοποίηση εννοιών-πληροφοριών και τη συσχέτιση-σύνδεση με άλλα ισχύοντα πρότυπα στον τομέα του CTI.

4.1 Ορισμός στόχων και απαιτήσεων

Οι βασικοί στόχοι που τέθηκαν για την δημιουργία ενός ολοκληρωμένου ταξινομικού συστήματος στα πλαίσια κοινοποίησης πληροφοριών των κυβερνοαπειλών είναι:

- Η δημιουργία ενός συγκεκριμένου πλαισίου εννοιών, το οποίο θα αποτελεί τον κεντρικό άξονα γύρω από τον οποίο θα έχει τη δυνατότητα να εκτυλίσσεται ένα κοινό λεξιλόγιο μεταξύ των λειτουργικών κέντρων ασφάλειας.
- Η ανάπτυξη μίας ευέλικτης και επεκτάσιμης οντολογίας για το CTI, βασισμένου στο μοντέλο SKOS, το οποίο περιλαμβάνει κατηγορίες όπως IoCs (Indicators of Comprise), Tactics techniques and procedures (TTPs), Vulnerabilities, Atomic Indicators, Courses of Actions, Targets μεταξύ άλλων.
- Η πιθανότητα διασύνδεσης του συστήματος με υπάρχοντα CTI πρότυπα όπως MITRE ATT&CK και STIX 2.0.
- Η υποστήριξη διαλειτουργικότητας με άλλα συναφή πληροφοριακά συστήματα κυβερνοασφάλειας.

4.2 Συλλογή και ανάπτυξη δεδομένων

Για τη δημιουργία της οντολογίας, πραγματοποιήθηκαν τα εξής βήματα:

- Διερεύνηση σχετικής βιβλιογραφίας με βάση λέξεις- κλειδιά όπως αναφέρονται στις συντομογραφίες.
- Μελέτη και συσχέτιση υπαρχόντων μοντέλων και προτύπων, όπως το MITRE ATT&CK, STIX 2.0, ISO 27001.
- Επεξεργασία και ανάλυση ιεραρχικά ταξινομημένων πληροφοριών που χρησιμοποιούνται στον τομέα του Cyber Threat Intelligence και το Cybersecurity γενικότερα.
- Επιλογή σχετικών εννοιών που αποτέλεσε χρήσιμο να συμπεριληφθούν στην οντολογία (πχ Identity, Motivation).
- Η αναζήτηση των πληροφοριών έγινε επιπλέον με βάση τις παραπάνω λέξεις κλειδιά σε ιστοσελίδες όπως google scholar, ieeexplrore (κ.α) βασιζόμενος σε άρθρα και papers παρόμοιου επιστημονικού πεδίου.
- Όσον αφορά την ανάπτυξη της οντολογίας αναζήτησα λεξικά παρόμοια σχετικά με το πεδίο της κυβερνοασφάλειας κυρίως από κρατικές ιστοσελίδες. Παρακάτω παρατίθενται ενδεικτικά κάποιες από αυτές:
  NICCS A Glossary of Common Cybersecurity Words and Phrases
  List of glossary terms used on cyber.gov.au website
  CISA Cyber Threats and Advisories
  NIST National Vulnerability Database
  NIST Glossary
  The National Cyber Security Centre
  ENISA Cyber Threats

COURSERA Cybersecurity Glossary: Key Terms & Definitions

* Επίσης αναζητήθηκαν πληροφορίες από ιστοσελίδες οργανισμών που κύριο στόχο έχουν την ενημέρωση γύρω από το θέμα τις κυβερνοασφάλειας καθώς και παρέχουν υπηρεσίες σε αυτό το πεδίο. Κάποιες εκ των οποίων είναι οι εξής:
  UKcybersecuritycouncil Glossary of cyber security terms
  Canadian Centre for Cyber Security Glossary
  Skillsoft Cybersecurity Glossary of Terms
  IBM Types of cyberthreats
  exabeam Cybersecurity Threats: Everything you Need to Know
  IBM What is red teaming?
  Zcybersecurity 4 types of Cyber Threat Intelligence Categorized

Αναλυτικότερες πληροφορίες σχετικά με τις παραπάνω ιστοσελίδες παρατίθενται στην βιβλιογραφία.
Άλλη πηγή από την οποία προέκυψαν σημαντικές πληροφορίες σχετικά με το αντικείμενο με το οποίο ασχολήθηκα στη παρούσα εργασία αποτέλεσε η συνέντευξη που πραγματοποιήθηκε διαδικτυακά με εξειδικευμένο προσωπικό στο τομέα της κυβερνοασφάλειας με σκοπό την ανατροφοδότηση και τον αναστοχασμό στο συγκεκριμένο ερευνητικό πεδίο. Παρακάτω παρατίθενται οι ερωτήσεις που πραγματοποιήθηκαν για τον παραπάνω σκοπό με τις απαντήσεις.

1. Have you worked with ontologies or semantic mapping before? a. If yes: how has this influenced your work? b. If no: how can this simplify knowledge or work in cybersecurity?
   Answer:

   Yes, I've had some exposure to ontologies and semantic mapping, primarily in the context of infrastructure documentation. For example, during audits or security assessments, having a semantically mapped model made it easier to trace dependencies and identify the potential impact of vulnerabilities. Basically, this means better correlation of logs and threat data across heterogeneous systems- be it a Linux sserver, a Windows server/endpoint, or an IBM AIX box running core services. Essentially, ontologies define relationships like "this server hosts this application, which connects to this database, which contains sensitive data". That model allows better risk analysis, automation in incident response, and more precise vulnerability management.

2. How do you identify and assess the different types of threats in the cybersecurity space?
   Answer:

   Usually I employ a multi-layered approach that integrates both technical indicators (e.g. CVEs) and higher-level threat modeling frameworks such as MITRE ATT&CK for adversary behavior analysis. Asset criticality and exposure are assessed in conjunction with threat data, often using a risk matrix informed by CVSS (Common Vulnerability Scoring System) scores and enriched through internal telemetry (e.g., SIEM logs , vulnerability scans). Semantic models, where available, enhance this by mapping assets to services and business impact, facilitating more accurate risk prioritization. This approach ensures that threat assessment is not merely reactive but strategically aligned with business context and evolving adversarial tactics.

3. What are the challenges in collecting and analyzing data to predict cyberattacks?
   Answer:

   Throughout my experience, I've noticed a major issue with data heterogeneity, as security-relevant data originates from diverse sources (e.g., logs, network flows, endpoint telemetry) with varying formats, semantics, and quality. Privacy and legal concerns also limit access to comprehensive datasets, particularly in regulated environments like banking or financial institutions. Usually, attackers deliberately manipulate data to evade detection, which further complicates prediction efforts.

4. How do you use information from cyber threat intelligence to enhance cybersecurity in an organization?
   Answer:

   Cyber Threat Intelligence enables the proactive identification of threats, the detection of attack patterns, and the anticipation of adversarial behavior. Practicallly, cyber threat intelligence is integrated into security operations to enrich SIEM alerts, drive incident response, and prioritize patching & mitigation efforts based on threat actor tactics and techniques. By mapping indicators of compromise with tactics, techniques, and procedures, I can contextualize threats relative to business impact, thereby improving response time and reducing false positives.

5. What tools and technologies do you consider essential for effective threat analysis and management?
   Answer:

   Essential tools and technologies that I consider essential for effective threat analysis are:
   -Security Information and Event Management (SIEM) platforms (e.g., Splunk) for centralized log aggregation, real-time correlation, and historical threat hunting.
   -Endpoint Detection and Response (EDR) solutions (e.g., CrowdStrike) to provide visibility and behavioral analysis at the endpoint level.
   -Threat Intelligence Platforms (TIPs) that aggregate and normalize threat feeds to enhance detection and inform proactive defenses.
   -Network Traffic Analysis (NTA) tools and IDS/IPS systems (e.g. Suricata, Snort) to monitor for anomalous behavior and lateral movement.
   -Security Orchestration, Automation, and Response (SOAR) platforms to enable faster, automated incident handling based on predefined playbooks.
   -Ontology-driven knowledge bases (e.g. MITRE) that standardize threat representation and enable semantic correlation across systems.
   Together, these technologies support the full threat lifecycle

6. How do you incorporate new and emerging technologies into your cyber threat intelligence strategy?
   Answer:
   Incorporating emerging technologies into a CTI strategy requires a structured, iterative approach that balances technological innovation with operational relevance. I adopt a multi-layered strategy consisting of three key components: continuous monitoring of technological trends, integration through pilot testing and threat modeling, and alignment with ontologies and automation frameworks for knowledge dissemination. Emerging technologies such as machine learning for anomaly detection, and structured

threat information formats like STIX/TAXII, are first evaluated against existing threat landscapes and infrastructure. Ontologies and semantic mapping are employed to ensure that the new data sources can be interpreted and correlated consistently across systems, enhancing interoperability and situational awareness.

7. How do you address the legal and regulatory challenges involved in collecting data for cyber threat intelligence?
   Answer:

   Addresing legal and regulatory challenges in cyber threat intelligence (CTI) collection requires a risk-aware, jurisdiction-specific approach that balances operational needs with compliance obligations. First, all data collection activities must align with applicable laws such as the General Data Protection Regulation (GDPR) in the EU, particularly when handling personally identifiable information (PII) or monitoring communications.
   Key strategies include:
   -Data minimization and anonymization to avoid processing unnecessary personal data.
   -Clear legal basis for data collection, often under legitimate interest or consent models.
   -Cross-border data governance, ensuring compliance with international transfer restrictions and third-party sharing frameworks.
   -Use of threat intelligence platforms (TIPs) that integrate legal controls, auditing, and classification of data sensitivity.
   Regular consultation with legal experts and Data Protection Officers (DPOs) is essential to validate practices, especially when leveraging open-source intelligence. Compliance must be embedded in CTI workflows through governance policies, audit mechanisms, and awareness of evolving legal standards.

8. How do you evaluate the effectiveness of the measures you take based on information from cyber threat intelligence?
   Answer:

   The effectiveness of measures derived from CTI is evaluated through a combination of quantitative and qualitative indicators. Key metrics include reduction in incident response time, improved detection rates, and the successful mitigation of known threats. Post-implementation assessments often involve simulated attacks to verify that CTI-informed controls effectively disrupt or detect relevant tactics and techniques.
   Additionally, feedback loops are established between threat detection systems, incident response teams, and threat intelligence sources to continuously assess the relevance and precision of the intelligence applied. Ontologies and structured threat models aid in aligning CTI with system-level knowledge.

9. Can you give us an example of a successful case where cyber threat intelligence significantly contributed to avoiding or mitigating a cyberattack?
   Answer:
   One notable example occurred during the WannaCry ransomware outbreak in 2017. We were able to identify the associated Indicators of Compromise (IOCs), including specific IP addresses, file hashes, and behaviors, before the attack reached our environments. For instance, shortly after the malware was discovered, CTI feeds and security communities shared knowledge of the “kill switch” domain that, when registered, effectively halted the spread of the ransomware. Similarly, other

"clone/branched" domains that came up later could be avoided in time through feeds and security communities.
Updating the detection systems, isolate vulnerable machines, and apply security patches quickly, prevented large-scale infection. This demonstrates how timely, actionable threat intelligence enables rapid defensive action, reducing both operational impact and financial loss.

10. What is your experience with CVEs (Common Vulnerabilities and Exposures)?
    Answer:

    Throughout my career managing heterogeneous infrastructures, including Linux, Windows, VMware, and IBM AIX systems. I have routinely worked with CVEs as part of vulnerability management and patching strategies. CVEs serve to me as a standardized reference for known security vulnerabilities, enabling consistent communication and assessment across tools and teams. In operational terms, I have used CVE data to prioritize remediation efforts based on CVSS scores, exploitability, and asset criticality. Integration with vulnerability scanners (e.g., OpenVAS) and SIEM tools has been central to identifying and tracking exposures in real-time. In regulated environments such as banking, CVE tracking was also integral to compliance reporting and audit readiness.
    Ontologically, CVEs may be incorporated into semantic models to enrich asset relationships with known threat intellligence, thereby enhancing situational awareness and automating risk analysis.

11. Why do you believe that vulnerabilities are difficult to manage and mitigate, even with the implementation of controls and best practices?
    Answer:

    Vulnerabilities remain difficult to manage and mitigate due to the dynamic and complex nature of modern IT environments. Even with controls and best practices in place, several factors contribute to persistent challenges:
    -Complex interdependencies: Modern systems are composed of heterogeneous platforms, legacy components, third-party software, and cloud services. Vulnerabilities in one layer can propagate through dependencies, making impact analysis and patching non-trivial.
    -Volume and velocity: The sheer number of newly discovered vulnerabilities, combined with the time required to test and deploy patches safely, often outpaces the capacity of operational teams.
    -Incomplete visibility: Asset discovery and inventory remain imperfect, especially in hybrid or decentralized infrastructures. Unknown or shadow systems often go unpatched.
    -Human factors: Misconfigurations, delayed patching, and inconsistent control enforcement due to resource or knowledge constraints undermine otherwise sound security practices.
    In essence, vulnerabilities are not just technical issues, but socio-technical challenges requiring integrated governance, automation, and continuous monitoring.

4.3 Ανάπτυξη της οντολογίας στο Protégé

Για την ανάπτυξη της οντολογίας επιλέχθηκε το Protege, ένα διαδεδομένο και αξιόπιστο εργαλείο μοντελοποίησης οντολογιών και αποτελεί ελεύθερο λογισμικό ανοιχτού κώδικα. Το Protege αναπτύσσεται και συντηρείται από το Stanford Center for Biomedical Informatics Research και χρησιμοποιείται τόσο στον ακαδημαϊκό όσο και στον επιχειρηματικό χώρο.

Η επιλογή του λογισμικού έγινε λόγω:

* Φιλικού περιβάλλοντος εργασίας (GUI) που καθιστά εύκολη δημιουργία και επεξεργασία εννοιών, σχέσεων και ιδιοτήτων.
* Υποστήριξης σε μοντέλα όπως OWL και SKOS, που το καθιστά ιδανικό για τη μοντελοποίηση περιεχομένου Σημασιολογικού Ιστού.
* Επέκτασης μέσω plugins, τα οποία προσφέρουν επιπλέον δυνατότητες όπως αυτόματο έλεγχο λειτουργικότητας, εισαγωγή δεδομένων και οπτικοποίηση των μοντέλων όπως Γράφοι.

Κατά τη διάρκεια της ανάπτυξης της οντολογίας, χρησιμοποιήθηκε το SKOS Vocabulary http://www.w3.org/2004/02/skos/core ως βάση μοντελοποίησης. Δημιουργήθηκαν έννοιες (skos:Concept) για τεχνικές απειλών και σχετικές έννοιες. Χρησιμοποιήθηκαν σχέσεις όπως skos:broader, skos:narrower, skos:related για την οργάνωση των πληροφοριών μέσα στην οντολογία. Η τεκμηρίωση των εννοιών έγινε με ετικέτες και ορισμούς όπως skos:prefLabel, skos:definition, skos:note.

Το Protege με την απλότητα του, βοήθησε αρκετά ως εργαλείο για την δημιουργία μιας δομημένης και επεκτάσιμης οντολογίας. Παρακάτω παρουσιάζονται τα βασικά βήματα που ακολουθήθηκαν:

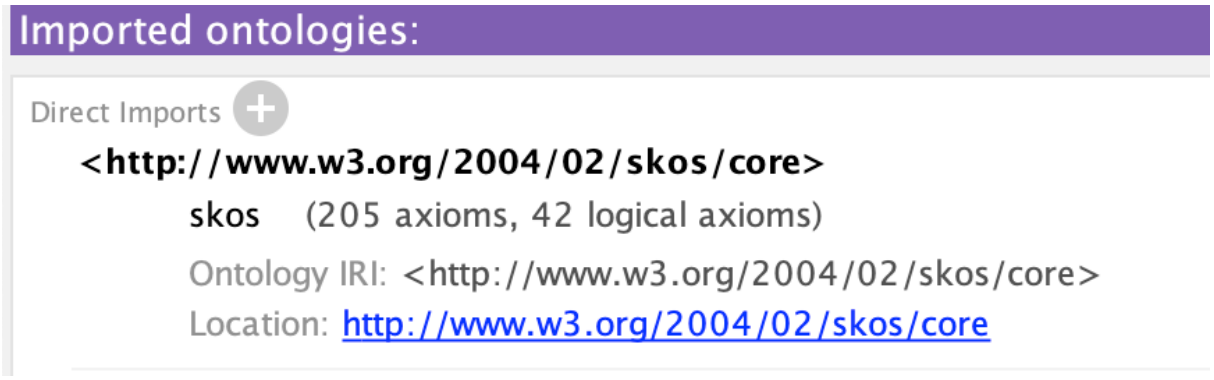
4.3.1 Εγκατάσταση και δημιουργία νέου Project

Χρησιμοποιήθηκε η έκδοση του Protege Desktop (5.6.4).

Έγινε εγκατάσταση των plugins: Protégé SKOS plugin στην έκδοση 1.2.0 για την δημιουργία της οντολογίας σε SKOS μοντέλο, του OntoGraf στην έκδοση 2.0.3 για την οπτικοποίηση του μοντέλου σε γράφο αναπαράστασης, ομοίως και το OWLViz στην έκδοση 5.0.3.

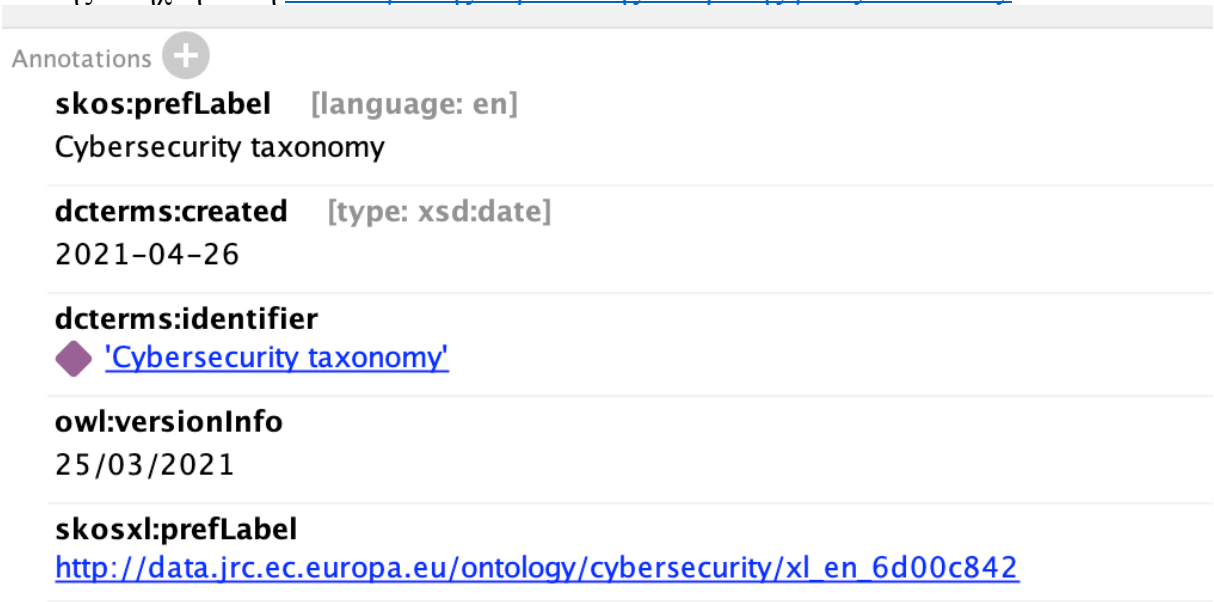
Δημιουργήθηκε νέο σχήμα σε OWL/RDF format με την ονομασία «CTI.skos» και υπέρ-σύνδεσμο Ontology IRI: http://www.semanticweb.org/paschalesmpekas/ontologies/2024/9/CTI.skos στον Σημασιολογικό Ιστό .

Εισήχθη το SKOS Vocabulary ως απαραίτητο για την οντολογία μας όπως φαίνεται στην παρακάτω εικόνα:



Εικόνα 10 - Imported Ontologies in Protégé

Επίσης εισήχθη και η Οντολογία της Ευρωπαϊκής Επιτροπής για cybersecurity:



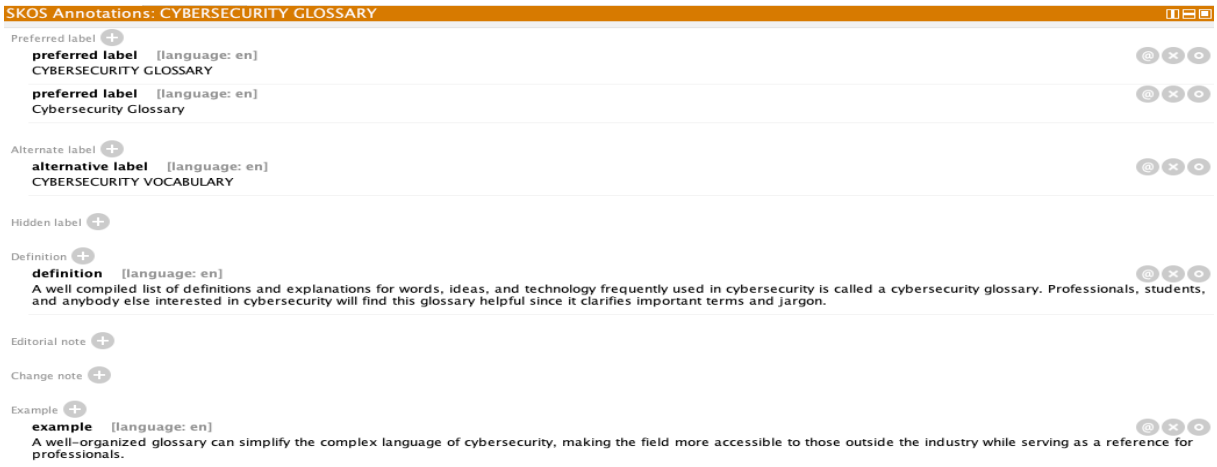
Εικόνα 11 - Εισαγωγή Cybersecurity Taxonomy της EU.

όπου έγιναν αρκετές συσχετίσεις των εννοιών με αυτές που δημιουργήσαμε με την χρήση σχέσεων χαρτογράφησης όπως skos:broadMatch, skos:closeMatch, skos:narrowMatch, skos:relatedMatch, για την ίσως μελλοντική διασύνδεση και αξιοποίηση τους.

4.3.2 Δημιουργία Κύριου Σχήματος

Ξεκινώντας την δημιουργία της οντολογίας, ακολουθήθηκε ένα μοντέλο συγγραφής αυτής, υιοθετώντας στοιχεία από 2 μοντέλα CTI που αναφερθήκαμε και ανωτέρω και συγκεκριμένα τα α) The Cyber Threat Intelligence (CTI) Model των Μαυροείδη Βασίλειου και Bromander Siri και β) Detection Maturity Level (DML) Model του Ryan Stillions.

Καταχωρήθηκε ένα skos:ConceptScheme με όνομα "CYBERSECURITY GLOSSARY" και ορίστηκε ως το βασικό σχήμα εννοιών της οντολογίας. Σε αυτό χρησιμοποιήθηκαν και άλλες SKOS ιδιότητες, όπου δηλώνουν την προτεινόμενη ονομασία του Σχήματος, την ενναλακτική του ονομασία, τον ορισμό του, μεταξύ άλλων:



Εικόνα 12 - Concept Scheme Annotations

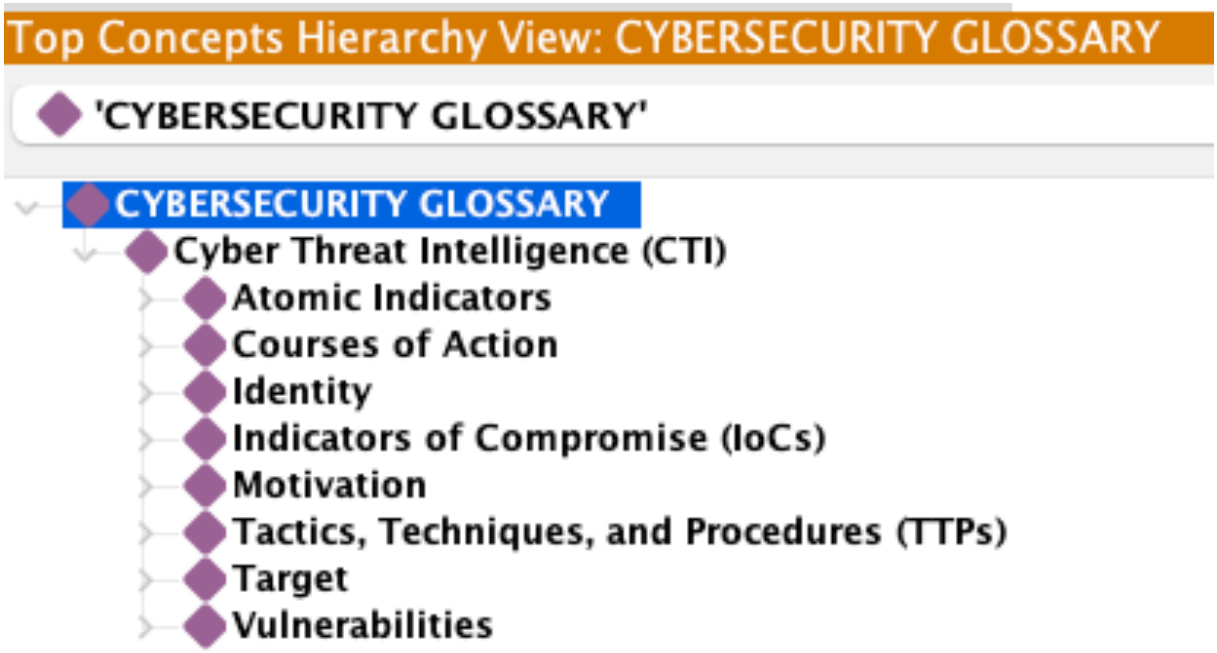
Έπειτα ορίστηκε το Top Concept του σχήματος, ένα skos:hasTopConcept με τις SKOS ιδιότητές του, με όνομα « Cyber Threat Intelligence (CTI) »:

Εικόνα 13 - Top Concept Annotations

Στη συνέχεια δημιουργήθηκαν οι κύριοι τομείς – έννοιες του μοντέλου μας με skos:narrower όπως:

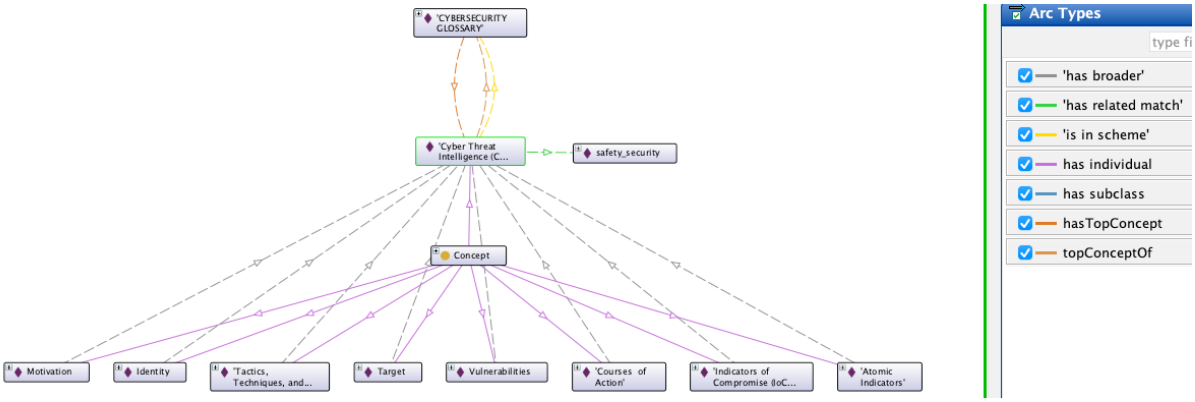
* Atomic Indicators
* Courses of Action
* Identity
* Indicators of Compromise (IoCs)
* Motivation
* Tactics, Techniques and Procedures (TTPs)
* Target
* Vulnerabilities

Η ιεραρχία του μοντέλου φαίνεται στην παρακάτω εικόνα:



Εικόνα 14 - Ιεραρχία CYBERSECURITY GLOSSARY

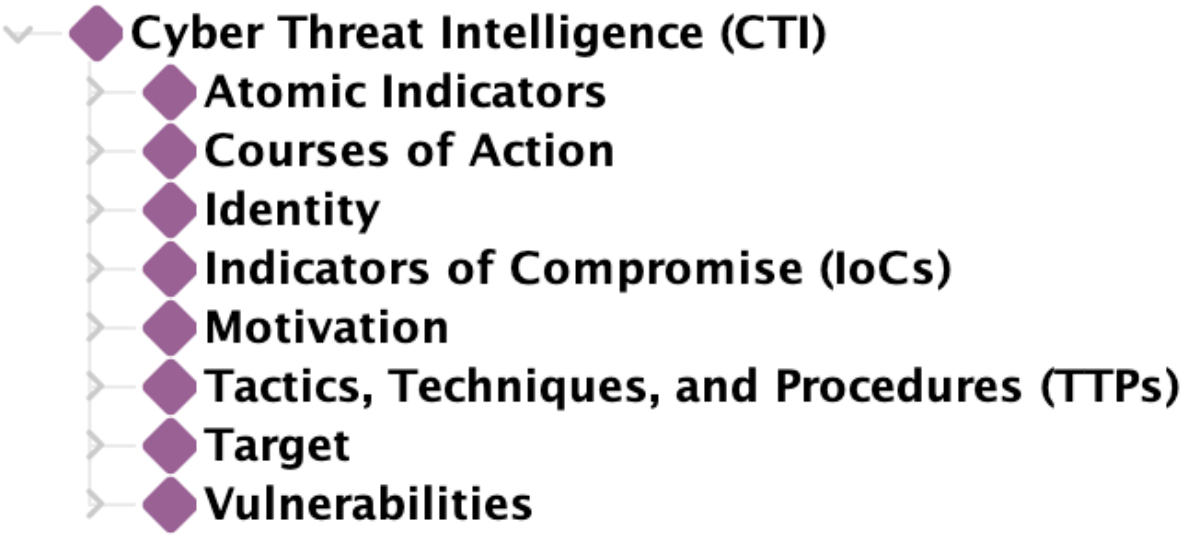
Με την βοήθεια του plugin OntoGraf του Protégé, παρουσιάζουμε την ιεραρχία και σε γράφο:



Εικόνα 15 - Ιεραρχία μοντέλου σε Γράφο.

4.3.3 Ορισμός Κύριων Εννοιών (Concepts)

Εδώ θα αναφερθούμε στις κύριες έννοιες-τομείς που δημιουργήθηκαν της οντολογίας μας με αλφαβητική σειρά όπως φαίνεται και από το παρακάτω απόσπασμα από το Protégé:

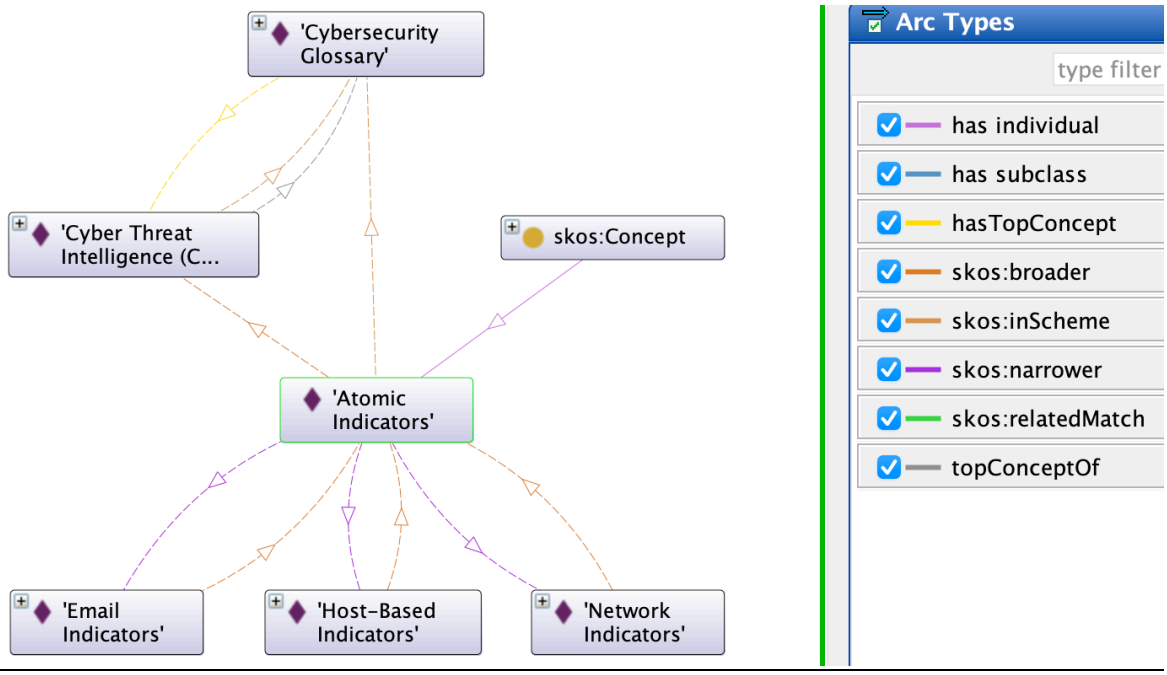


Εικόνα 16 - Κύριες έννοιες-τομείς οντολογίας

Για τις έννοιες (Concepts): Atomic Indicators, Courses of Actions, Identity, Indicators of Compromise (IoCs), Motivation, Tactics, Techniques and Procedures (TTPs), Target, αναφερθήκαμε στο κεφάλαιο 2.4.4 του The Cyber Threat Intelligence (CTI) Model των Μαυροείδη και Bromander (Bromander 2017).

Atomic Indicators
Όπως αναφερθήκαμε και προηγουμένως, είναι βασικά στοιχεία αναγνώρισης απειλών, όπως IP διευθύνσεις, ονόματα παρόχων (domains), hashes αρχείων, έχουν μικρή διάρκεια ζωής, καθώς οι επιτιθέμενοι μπορούν εύκολα να τα αλλάξουν. Στην εικόνα διακρίνουμε τον γράφο αυτού του concept με την ιεραρχία του και με ιδιότητα skos:narrower έχει τις εξής έννοιες:

- *Email Indicators*: Πρόκειται για δείκτες που έχουν σχέση με ύποπτα ή κακόβουλα email, όπως διευθύνσεις, domains, ή θεματικές γραμμές. Μας βοηθούν να εντοπίσουμε phishing ή spam προσπάθειες από την πρώτη ματιά. Ένα παράδειγμα μπορεί να είναι ένα email που έρχεται από «support@googLe.com» (με το "L" να είναι κεφαλαίο αντί για μικρό).
- *Host-Based Indicators*: Πρόκειται για δείκτες που μπορεί να εντοπιστούν στο σύστημα του θύματος, όπως file hashes, paths ή registry changes. Χρησιμεύουν στον εντοπισμό κακόβουλης δραστηριότητας μετά από μία εισβολή. Ένα παράδειγμα μπορεί να είναι ένα αρχείο με hash που ταιριάζει με ένα γνωστό malware ή μια αλλαγή στο registry file που δείχνει εγκατάσταση ενός keylogger (ανιχνευτής πλήκτρων).
- *Network Indicators:* Πρόκειται για δείκτες που βασίζονται στην κυκλοφορία δεδομένων στο δίκτυο, όπως IP διευθύνσεις, URLs ή domains που χρησιμοποιούνται για επιθέσεις. Ένα παράδειγμα μπορεί να είναι μια IP διεύθυνση που συνδέεται επανειλημμένα με γνωστά botnets ή μια διεύθυνση που οδηγεί σε σελίδα εγκατάστασης κακόβουλου λογισμικού.



Εικόνα 17 - Atomic Indicators Concept

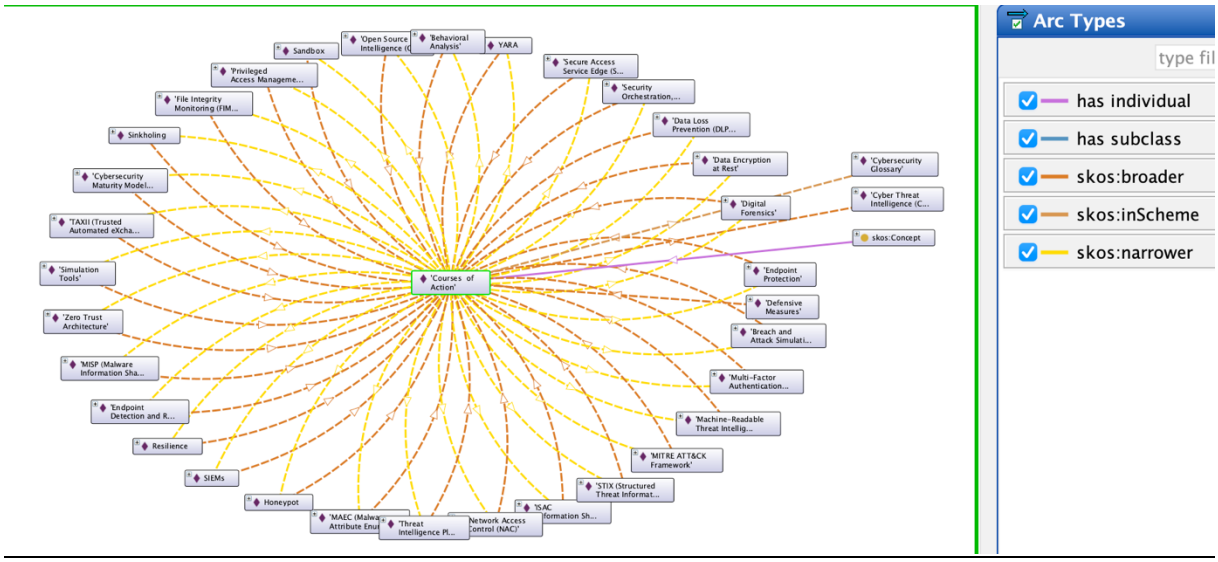
Courses of Actions

Αναφερόμενοι και ανωτέρω, τα Σχέδια Δράσης περιλαμβάνουν τα μέτρα που μπορούν να ληφθούν για την πρόληψη ή την αντιμετώπιση ενάντια σε κυβερνοεπιθέσεις. Τέτοια μέτρα συμπεριλάβαμε στην οντολογία μας όπως αναφέρονται και παρακάτω:

- *Behavioral Analysis:* Έννοια για την ανάλυση της συμπεριφοράς χρηστών ή των συστημάτων αυτών για τον εντοπισμό ύποπτων ενεργειών.
- *Breach and Attack Simulation (BAS): Έννοια για την* προσομοίωση επιθέσεων και τον εντοπισμό ευπαθειών στην άμυνα του συστήματος.
- *Cybersecurity Maturity Model Certification (CMMC):* Έννοια για την αξιολόγηση της ωριμότητας ενός οργανισμού στον τομέα της κυβερνοασφάλειας.
- *Data Encryption at Rest*: Έννοια για την κρυπτογράφηση δεδομένων που είναι αποθηκευμένα ψηφιακά μέσα όπως σκληρούς δίσκους ή βάσεις δεδομένων.
- *Data Loss Prevention (DLP):* Έννοια για τα μέτρα που μπορούν να αποτρέπουν τη διαρροή ευαίσθητων δεδομένων (email, cloud, USB).
- *Defensive Measures:* Έννοια για τα μέτρα προστασίας, όπως firewalls, antivirus, monitoring εργαλείων.
- *Digital Forensics*: Έννοια για την ανάλυση ψηφιακών στοιχείων μετά από περιστατικά επιθέσεων στην ασφάλεια των συστημάτων για την εύρεση των αιτίων.
- *Endpoint Detection and Response (EDR):* Έννοια για βοηθητικό λογισμικό ανίχνευσης και ενεργειών αντιμετώπισης απειλών σε τερματικά συστήματα.
- *Endpoint Protection:* Έννοια για την ολοκληρωμένη προστασία συσκευών από malware και άλλες παρόμοιες εισβολές.
- *File Integrity Monitoring (FIM):* Έννοια για την παρακολούθηση αρχείων μέσα στο σύστημα για ύποπτες ή μη εξουσιοδοτημένες ενέργειες ή αλλαγές.
- *Honeypot*: Έννοια για ένα σύστημα-παγίδα που χρησιμοποιείται για την παρακολούθηση των επιθέσεων.
- *ISAC (Information Sharing and Analysis Center):* Έννοια για τα κέντρα που διευκολύνουν την διασύνδεση και ανταλλαγή πληροφοριών ασφαλείας.

- *Machine-Readable Threat Intelligence (MRTI):* Έννοια για τα δεδομένα απειλών σε μορφή που είναι κατανοητή από το σύστημα και το λογισμικό.
- *MAEC:* Έννοια για την περιγραφή χαρακτηριστικών κακόβουλου λογισμικού.
- *MISP*: Έννοια για μία πλατφόρμα για την ανταλλαγή δεδομένων κυρίως για malware και άλλες απειλές.
- *MITRE ATT&CK Framework:* Έννοια για την πλατφόρμα όπου είναι ένα λεξικό με τεχνικές που χρησιμοποιούν οι επιτιθέμενοι, αλλά και για την ανάλυση των απειλών.
- *Multi-Factor Authentication (MFA):* Έννοια για την ταυτοποίηση με πάνω από ένα επίπεδο ελέγχου (2FA).
- *Network Access Control (NAC*): Έννοια για τον έλεγχο εισόδου-εξόδου σε ένα δίκτυο.
- *Open Source Intelligence (OSINT):* Έννοια για τις πληροφορίες που συγκεντρώνονται από δημόσιες πηγές (social media).
- *Privileged Access Management (PAM*): Έννοια για την διαχείριση των λογαριασμών ενός συστήματος με admin δικαιώματα για την αποφυγή κατάχρησης των δικαιωμάτων.
- *Resilience*: Έννοια για την ικανότητα ενός οργανισμού να διατηρεί τη λειτουργία του ακόμα και αν βρίσκεται εν μέσω περιόδου επίθεσης.
- *Sandbox*: Έννοια για ένα αποστειρωμένο περιβάλλον για την ασφαλή εκτέλεση και ανάλυση κακόβουλου λογισμικού.
- *Secure Access Service Edge (SASE):* Έννοια για τον συνδυασμό δικτύωσης και ασφάλειας μέσω cloud τεχνολογιών.
- *Security Orchestration, Automation, and Response (SOAR):* Έννοια για την ενοποίηση και αυτοματοποίηση ενεργειών απόκρισης σε περιστατικά επιθέσεων.
- *SIEMs:* Έννοια για εργαλεία που συλλέγουν και αναλύουν logs για την ανίχνευση απειλών και την παρακολούθηση ανάλογων συμβάντων.
- *Simulation Tools:* Έννοια για εργαλεία που δημιουργούν προσομοίωση επιθέσεων για εκπαιδευτικούς και σκοπούς αξιολόγησης.
- *Sinkholing*: Έννοια για την τεχνική που ανακατευθύνει την κακόβουλη επίθεση σε ένα ασφαλές περιβάλλον για την παρακολούθηση της.
- *STIX:* Έννοια για το πρότυπο τυποποιημένης καταγραφής και αναπαράστασης πληροφοριών των απειλών.
- *TAXII:* Έννοια για το πρωτόκολλο ασφαλούς και αυτοματοποιημένης ανταλλαγής πληροφοριών των απειλών μεταξύ πληροφοριακών συστημάτων.
- *Threat Intelligence Platforms (TIPs):* Έννοια για τα πλατφόρμες συγκέντρωσης και διαχείρισης πληροφοριών των απειλών από πολλές και διαφορετικές πηγές.
- *YARA*: Έννοια για τον ορισμό κανόνων εντοπισμού κακόβουλου λογισμικού σε αρχεία ή στην μνήμη του συστήματος.
- *Zero Trust Architecture:* Έννοια για ένα μοντέλο ασφαλείας που «δεν εμπιστεύεται τίποτα και κανέναν» χωρίς να περάσει από έλεγχο και κάθε πρόσβαση σε αυτό επαληθεύεται.

Στην εικόνα διακρίνουμε τον γράφο αυτού του concept με την ιεραρχία του και με ιδιότητα skos:narrower:



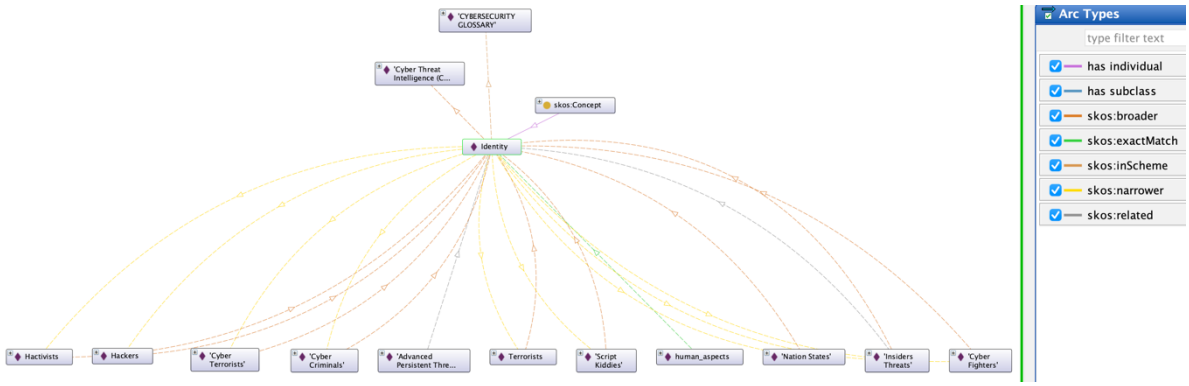
Εικόνα 18 - Courses of Actions

Identity

Η ταυτότητα ενός επιτιθέμενου (Threat Actor) όπως αναφερθήκαμε και πριν, μπορεί να είναι η ονομασία του, η ονομασία μιας οργάνωσης ή ακόμη και ενός κράτους. Παρακάτω αναφέρουμε τις έννοιες αυτού του concept όπως αναφέρονται και παρακάτω:

- *Cyber Criminals*: Έννοια για άτομα ή ομάδες αυτών που πραγματοποιούν επιθέσεις με κύριο στόχο το χρηματικό όφελος, από απάτες, ή κλοπή δεδομένων κ.α.
- *Cyber Fighters*: Έννοια για επιτιθέμενους που δρουν με ιδεολογικά κριτήρια ή υποκινούμενοι από εθνικά συμφέροντα, με στόχο να υπερασπιστούν ή να προωθήσουν κάποιο σκοπό στον κυβερνοχώρο.
- *Cyber Terrorists*: Έννοια για χρήστες ή ομάδες αυτών που πραγματοποιούν τρομοκρατικές ενέργειες μέσω του διαδικτύου, με στόχο να προκαλέσουν φόβο, κοινωνική αναταραχή ή να ασκήσουν πίεση σε κυβερνήσεις.
- *Hackers*: Έννοια για άτομα με γνώσεις προγραμματισμού και ασφάλειας που εισέρχονται σε συστήματα, είτε για εξερεύνηση, είτε για κακόβουλες ενέργειες.
- *Hactivists*: Έννοια για χάκερς με ακτιβιστικά κίνητρα που επιτίθενται σε συστήματα για να προβάλουν πολιτικά, κοινωνικά ή ηθικά μηνύματα (Anonymous).
- Insiders Threats: Έννοια για απειλές που προέρχονται από ενδότερους χρήστες ενός οργανισμού, όπως υπάλληλοι ή άτομα με πρόσβαση σε κρίσιμα δεδομένα.
- *Nation States*: Έννοια για κυβερνήσεις ή υποστηριζόμενες ομάδες που πραγματοποιούν οργανωμένες κυβερνοεπιθέσεις για κατασκοπία ή άλλη επιρροή.
- *Script Kiddies*: Έννοια για άπειρους ή αρχάριους χρήστες που χρησιμοποιούν έτοιμα εργαλεία και scripts χωρίς ιδιαίτερη τεχνική γνώση πού πολλές φορές πραγματοποιούνται για λόγους επίδειξης ή διασκέδασης.
- *Terrorists*: Γενική έννοια για άτομα ή ομάδες που χρησιμοποιούν τον κυβερνοχώρο για να υποστηρίξουν ή ενισχύσουν τρομοκρατικές ενέργειες.

Στην εικόνα διακρίνουμε τον γράφο αυτού του concept με την ιεραρχία του και με ιδιότητα skos:narrower:



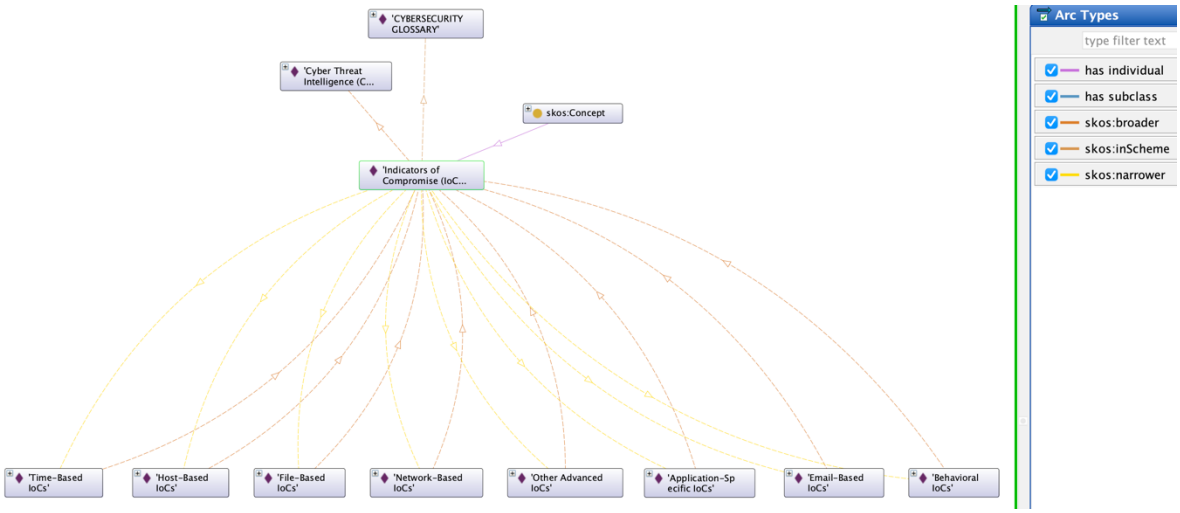
Εικόνα 19 - Identity

Indicators of Compromise (IoCs)

Σε προηγούμενη αναφορά, είδαμε πως πρόκειται για στοιχεία που βοηθούν στην ανίχνευση κακόβουλων δραστηριοτήτων και στην ταυτοποίηση συγκεκριμένων μοτίβων επιθέσεων. Παρακάτω αναφέρουμε τις έννοιες αυτού του concept όπως:

- Application-Specific IoCs: Έννοια για δείκτες που σχετίζονται με συγκεκριμένες εφαρμογές, όπως logs, συμπεριφορά ή αρχεία ρυθμίσεων που προϊδεάζουν σε κακόβουλη δραστηριότητα.
- Behavioral IoCs: Έννοια για ενδείξεις συμπεριφοράς ενός χρήστη ή ενός συστήματος, όπως ξαφνικές αλλαγές, αυτοματοποιημένες ενέργειες ή μη συνηθισμένες ενέργειες.
- Email-Based IoCs: Έννοια για δείκτες που εντοπίζονται σε ύποπτα emails, π.χ. διευθύνσεις, συνημμένα ή domains σε υπερσυνδέσμους (links).
- File-Based IoCs: Έννοια που αφορά αρχεία ύποπτα, όπως file hashes (MD5, SHA256), ονόματα αρχείων ή συγκεκριμένες διαδρομές εγκατάστασης ενός malware.
- Host-Based IoCs: Έννοια για δείκτες που εντοπίζονται σε έναν υπολογιστή, όπως αλλαγές στο registry, στα services ή τροποποιήσεις αρχείων συστήματος.
- Network-Based IoCs: Έννοια για δείκτες που σχετίζονται με την κίνηση στο διαδίκτυο, όπως IPs, domains, ports ή URLs που χρησιμοποιούνται κυρίως για την επικοινωνία με τους επιτιθέμενους.
- Other Advanced IoCs: Έννοια για σύνθετους δείκτες που συνδυάζουν πολλές πηγές ή προέρχονται από την διαδικασία machine learning, threat intelligence feeds ή custom rules.
- Time-Based IoCs: Έννοια για δείκτες που σχετίζονται με χρονική σφραγίδα, όπως συγκεκριμένες ώρες εκτέλεσης επιθέσεων, patterns που εμφανίζονται σε συγκεκριμένα διαστήματα.

Στην εικόνα διακρίνουμε τον γράφο αυτού του concept με την ιεραρχία του και με ιδιότητα skos:narrower:



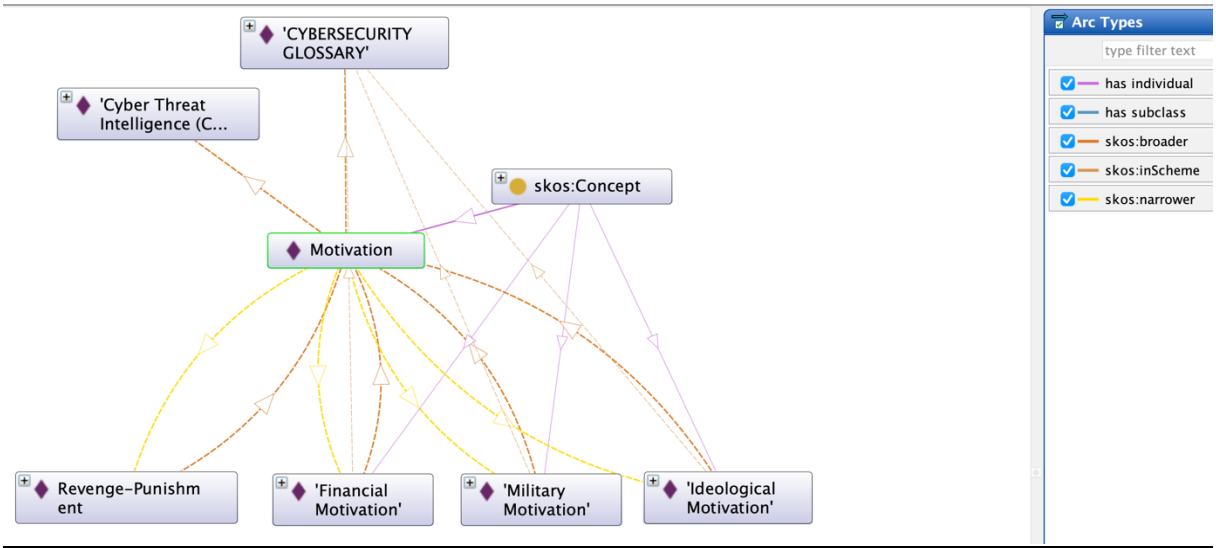
Εικόνα 20 - Indicators of Compromise (IoCs).

Motivation

Με το κίνητρο που αναφερθήκαμε προηγουμένως στο κεφάλαιο 2.4.4 του The Cyber Threat Intelligence (CTI), είναι αυτό που οδηγεί έναν επιτιθέμενο να πραγματοποιήσει μια ενέργεια είτε κακόβουλη είτε όχι, με σκοπό την επίτευξη συγκεκριμένων στόχων προσωπικών ή μη. Συνήθως, το κίνητρο σχετίζεται με τα οφέλη που αποκομίζει ο επιτιθέμενος από την επίτευξη των στόχων που έχει θέσει .Παρακάτω αναφέρουμε τις έννοιες αυτού του concept όπως:

- Financial Motivation: Έννοια για επιθέσεις με στόχο το χρηματικό όφελος, όπως με τεχνικές ransomware, phishing ή τραπεζικές απάτες.
- Ideological Motivation: Έννοια για το κίνητρο που βασίζεται σε πολιτικές, θρησκευτικές ή κοινωνικές πεποιθήσεις.
- Military Motivation: Έννοια για επιθέσεις που έχουν κύριο στόχο την στρατηγική υπεροχή ή κατασκοπία από κα προς στρατιωτικούς ή κρατικούς στόχους.
- Revenge–Punishment: Έννοια για επιθέσεις που γίνονται με σκοπό την εκδίκηση ή για να «τιμωρηθεί» κάποιος οργανισμός (π.χ. από πρώην υπάλληλο).

Στην εικόνα διακρίνουμε τον γράφο αυτού του concept με την ιεραρχία του και με ιδιότητα skos:narrower:



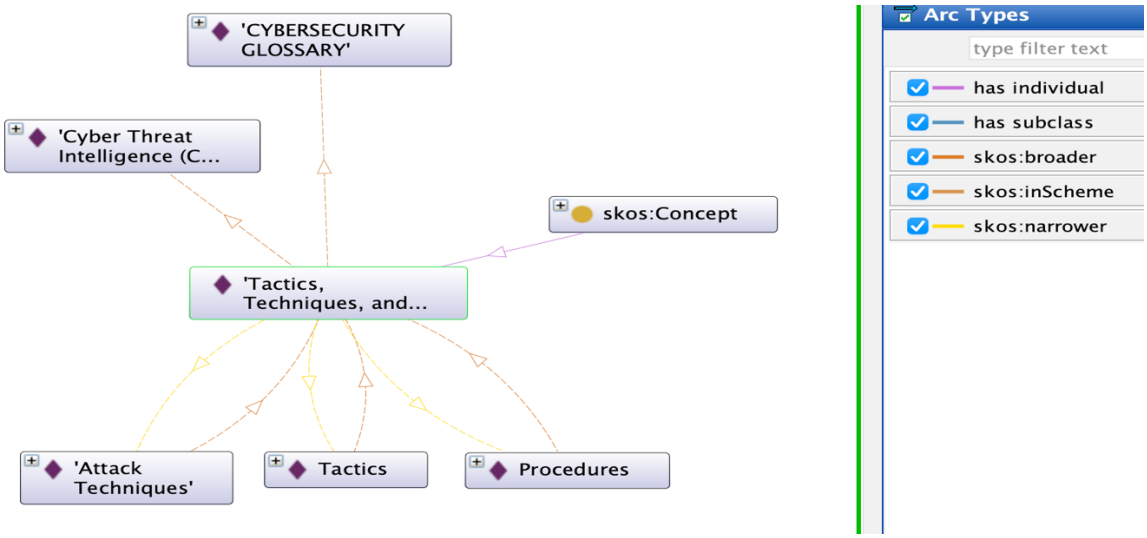
Εικόνα 21 – Motivation

Tactics, Techniques and Procedures (TTPs)

Πρόκειται όπως αναφερθήκαμε, σε τακτικές, τεχνικές και διαδικασίες που περιγράφουν τη συμπεριφορά των επιτιθέμενων με βάση:

- Τι κάνουν (Tactics).
- Πώς το κάνουν (Techniques).
- Ποια ακριβώς τα βήματα που ακολουθούν (Procedures).

Στην εικόνα διακρίνουμε τον γράφο αυτού του concept με την ιεραρχία του και με ιδιότητα skos:narrower:



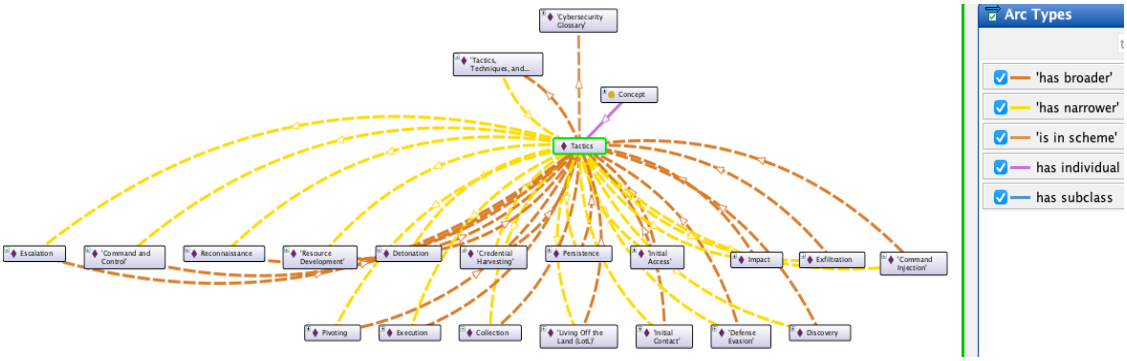
Εικόνα 22 - TTPs

Παρακάτω αναφέρουμε τις έννοιες αυτού του concept όπως:

- *Tactics*: Έννοια για το «τι» προσπαθεί να πετύχει ο επιτιθέμενος όπως πρόσβαση σε ένα πληροφοριακό σύστημα, εξαγωγή δεδομένων ή παραμονή σε αυτό. «Παιδία» αυτού του concept, δημιουργήθηκαν όπως:
  - Collection: Έννοια για την συλλογή δεδομένων από το σύστημα του θύματος, όπως αρχεία, credentials ή emails.
  - Command and Control: Έννοια για την δημιουργία δίαυλου επικοινωνίας με το μολυσμένο σύστημα για απομακρυσμένο έλεγχο.
  - Command Injection: Έννοια για την εκτέλεση κακόβουλων εντολών σε σύστημα όπως μία φόρμα συμπλήρωσης στοιχείων.
  - Credential Harvesting: Έννοια για την κλοπή στοιχείων ταυτότητας των χρηστών.
  - Defense Evasion: Έννοια για τις τεχνικές και την αποφυγή ανίχνευσης από μηχανισμούς ασφαλείας όπως antivirus, firewalls.
  - Detonation: Έννοια για την ενεργοποίηση κακόβουλου φόρτου (payload) στον στόχο.
  - Discovery: Έννοια για την χαρτογράφηση του συστήματος του χρήστη πριν από μία επίθεση.
  - Escalation: Έννοια για την απόκτηση πλήρη δικαιωμάτων σε ένα σύστημα.
  - Execution: Έννοια για την εκτέλεση κακόβουλου κώδικα.
  - Exfiltration: Έννοια για την κρυφή μεταφορά αποσπώμενων δεδομένων εκτός δικτύου.
  - Impact: Έννοια για την καταστροφή, τροποποίηση ή χειραγώγηση δεδομένων ή συστημάτων γενικά.
  - Initial Access: Έννοια για την πρώτη πρόσβαση στο σύστημα μέσω phishing, malware ή διάφορων exploits.

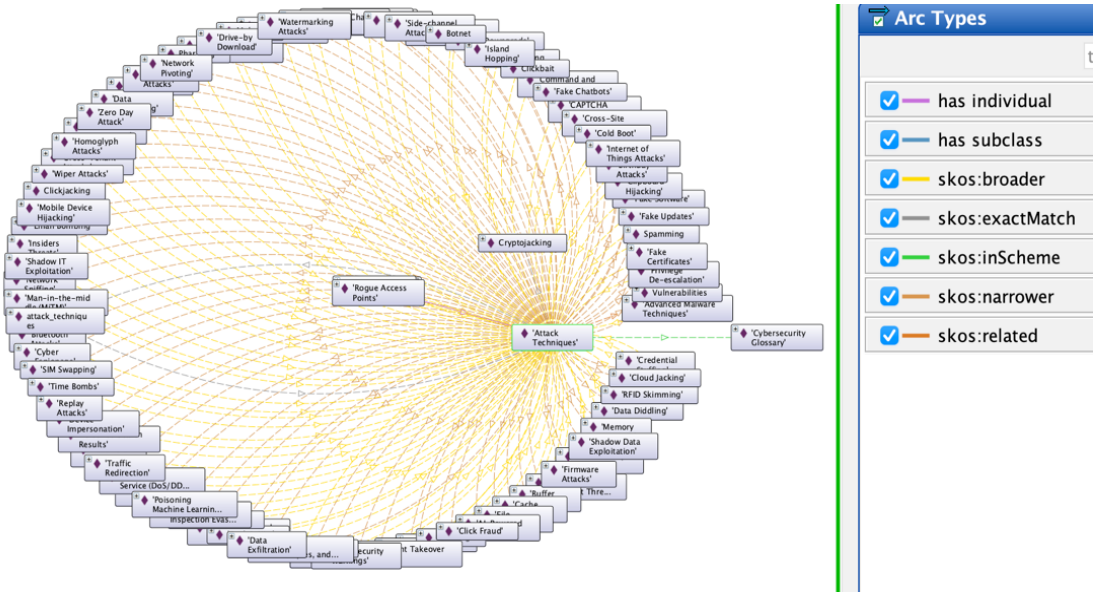
- Initial Contact: Έννοια για την πρώτη επαφή με το υποψήφιο θύμα (όπως phishing email, SMS).
- Living Off the Land (LoL): Έννοια για την χρήση υπαρχόντων εργαλείων του λειτουργικού συστήματος για επίθεση (όπως το PowerShell).
- Persistence: Έννοια για την παραμονή στο σύστημα από τον επιτιθέμενο, παρά τις προσπάθειες καθαρισμού ή επανεκκίνησης.
- Pivoting: Έννοια για την χρήση ενός ήδη μολυσμένου συστήματος για την πρόσβαση σε άλλα συστήματα μέσα στο δίκτυο.
- Reconnaissance: Έννοια για την έρευνα και συλλογή πληροφοριών για τον στόχο πριν κάποια επίθεση.
- Resource Development: Έννοια για την κατασκευή ή προμήθεια εργαλείων, ταυτοτήτων που θα χρησιμοποιηθούν στην επίθεση.

Στην εικόνα διακρίνουμε τον γράφο αυτού του concept με την ιεραρχία του και με ιδιότητα skos:narrower:



Εικόνα 23 - Tactics

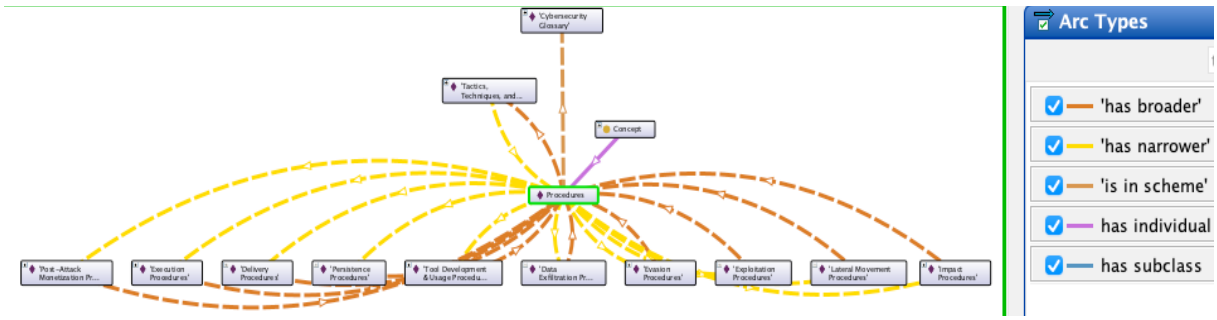
- *Attack Techniques*: Έννοια για το «πώς» γίνεται μία επίθεση και οι συγκεκριμένες τεχνικές που ακολουθούν όπως Phishing techniques, Malware, Spoofing, Spamming και πολλές άλλες. Οι συγκεκριμένες τεχνικές που συλλέχθηκαν και αποτυπώθηκαν ως έννοιες στην οντολογία μας, λόγω του μεγάλου όγκου αυτών, δεν μπορούν να αναφερθούν εδώ. Ακολουθεί ένα στιγμιότυπο σε γράφο παρουσιάζοντας ένα απόσπασμα αυτών:



Εικόνα 24 - Attack Techniques

- *Procedures*: Έννοια για το πλάνο που ακολουθεί ο επιτιθέμενος για να υλοποιήσει μια τεχνική επίθεσης (όπως scripts, διάφορα εργαλεία ανάλογων επιθέσεων, άλλες παραλλαγές των προηγούμενων).
    - Data Exfiltration Procedures: Έννοια για τους τρόπους εξαγωγής δεδομένων από το δίκτυο του θύματος χωρίς να γίνει αντιληπτό.
    - Delivery Procedures: Έννοια για τις μεθόδους μεταφοράς κακόβουλου φόρτου στο θύμα (όπως malvertising).
    - Evasion Procedures: Έννοια για τις διαδικασίες ώστε να περάσει η κακόβουλη δραστηριότητα απαρατήρητη από τα συστήματα ασφαλείας.
    - Execution Procedures: Έννοια για τα βήματα ενεργοποίησης του κακόβουλου κώδικα.
    - Exploitation Procedures: Έννοια για τις ενέργειες που εκμεταλλεύονται ευπάθειες στο λογισμικό ή το λειτουργικό σύστημα.
    - Impact Procedures: Έννοια για τις διαδικασίες που προκαλούν ζημιά στο στόχο, όπως διαγραφή αρχείων, κρυπτογράφηση δεδομένων (ransomware).
    - Lateral Movement Procedures: Έννοια για τις τεχνικές που χρησιμοποιεί ο επιτιθέμενος για να μετακινηθεί από ένα σύστημα σε ένα άλλο μέσα στο δίκτυο.
    - Persistence Procedures: Έννοια για τις ενέργειες ώστε να εξασφαλιστεί ότι θα διατηρηθεί η πρόσβαση ακόμα και μετά από επανεκκίνηση ή ενημέρωση του συστήματος.
    - Post-Attack Monetization Procedures: Έννοια για τις διαδικασίες που γίνονται για την εκμετάλλευση των αποτελεσμάτων της επίθεσης όπως πώληση δεδομένων ή ζητώντας λύτρα.
    - Tool Development and Usage Procedures: Έννοια για την ανάπτυξη ή χρήση ειδικών εργαλείων για να διευκολυνθούν άλλες φάσεις των επιθέσεων.

Στην εικόνα διακρίνουμε τον γράφο αυτού του concept με την ιεραρχία του και με ιδιότητα skos:narrower:



Εικόνα 25 - Procedures

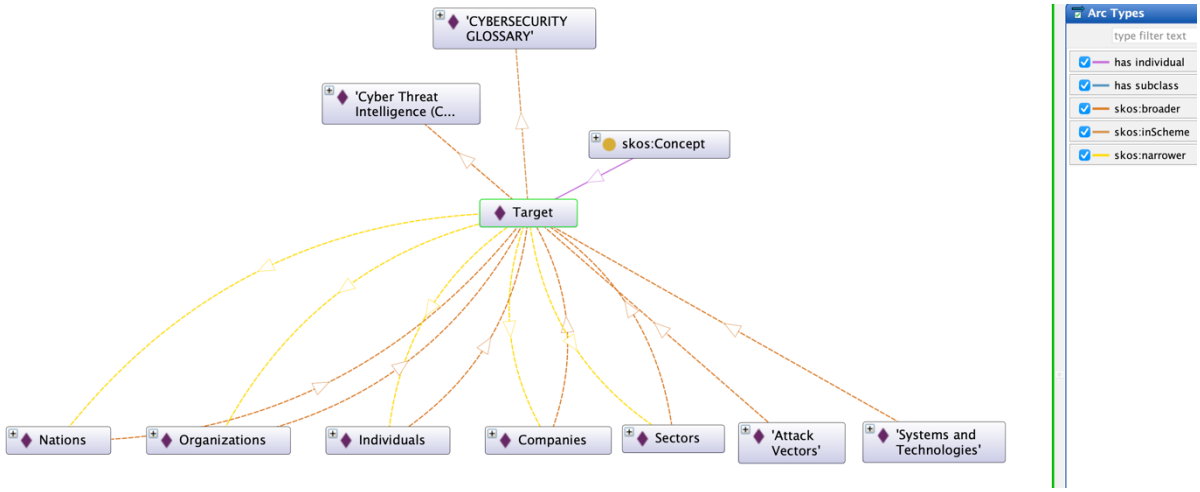
Target

Ο στόχος περιλαμβάνει το τελικό αποτέλεσμα που επιδιώκεται, καθώς και τα μέσα και τις ενέργειες που απαιτούνται για την επίτευξή του. Παρακάτω αναφέρουμε τις έννοιες αυτού του concept όπως:

- Attack Vectors: Έννοια για τα βήματα που χρησιμοποιεί μια τεχνική επίθεσης για να διεισδύσει σε ένα σύστημα.
- Companies: Έννοια για τις ιδιωτικές επιχειρήσεις ή οργανισμούς ως στόχος (συνήθως για οικονομικό ή ανταγωνιστικό όφελος).

- Individuals: Έννοια για τα στελέχη οργανισμών, υπάλληλοι, ή απλοί χρήστες –που μπορεί να γίνουν στόχοι επιθέσεων phishing, social engineering κ.α.
- Nations: Έννοια για κράτη που αποτελούν στόχους κατασκοπείας ή κυβερνοεπιθέσεων.
- Organizations: Έννοια για μηχανισμούς όπως ΜΚΟ, ερευνητικά ιδρύματα ή άλλες κρατικές υπηρεσίες.
- Sectors: Έννοια για ολόκληρους τομείς οικονομίας ή τεχνολογίας (όπως ενέργεια, υγεία, χρηματοοικονομικά).
- Systems and Technologies: Έννοια για πλατφόρμες, λειτουργικά συστήματα, βάσεις δεδομένων, IoT κ.α.

Στην εικόνα διακρίνουμε τον γράφο αυτού του concept με την ιεραρχία του και με ιδιότητα skos:narrower:



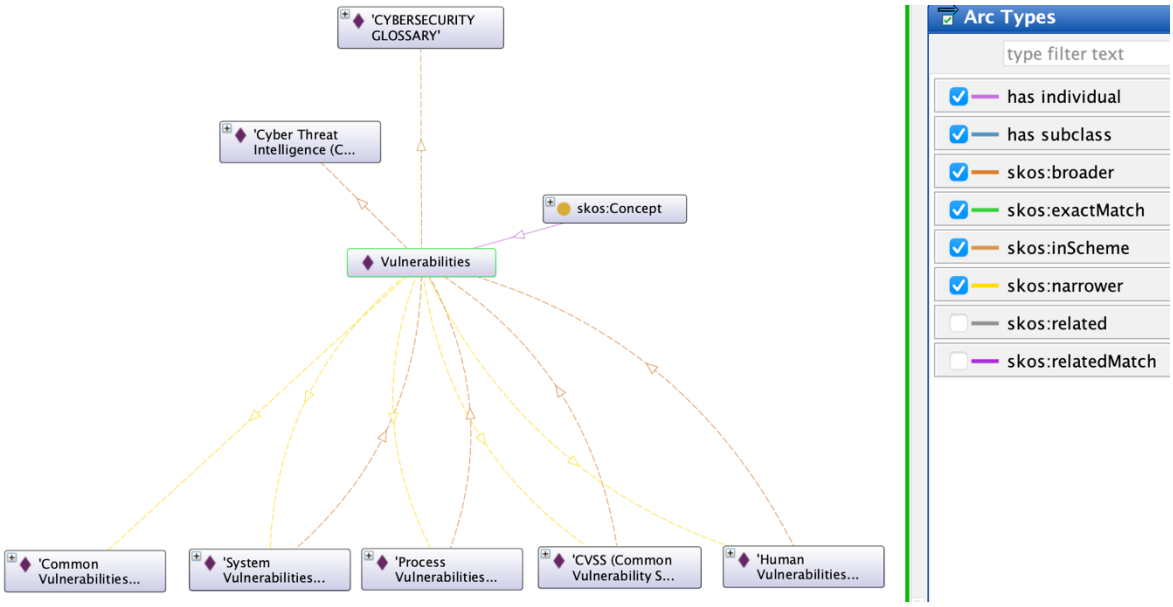
Εικόνα 26 – Target

Vulnerabilities

Οι ευπάθειες αποτελούν κρίσιμη παράμετρο κατανόησης του κινδύνου που απειλεί έναν οργανισμό ή ένα πληροφοριακό σύστημα. Μια ευπάθεια μπορεί να προέρχεται τόσο από τεχνικές αδυναμίες στα πληροφοριακά συστήματα, όσο και από ανθρώπινα λάθη. Παρακάτω αναφέρουμε τις έννοιες αυτού του concept όπως:

- Common Vulnerabilities and Exposures (CVE): Έννοια για τις καταγεγραμμένες ευπάθειες λογισμικού.
- CVSS (Common Vulnerability Scoring System): Έννοια για ένα σύστημα που βαθμολογεί την επικινδυνότητα μιας ευπάθειας, σε κλίμακα από 0 έως 10.
- Human Vulnerabilities: Έννοια για τα τρωτά σημεία που οφείλονται σε ανθρώπινο παράγοντα, όπως κακή εκπαίδευση ή phishing.
- Process Vulnerabilities: Έννοια για τις αδυναμίες ενός οργανισμού.
- System Vulnerabilities: Έννοια για τα τεχνικά σφάλματα ή τις παραλείψεις στα πληροφοριακά συστήματα ή το λογισμικό που τα καθιστούν ευάλωτα σε επιθέσεις.

Στην εικόνα διακρίνουμε τον γράφο αυτού του concept με την ιεραρχία του και με ιδιότητα skos:narrower:



Εικόνα 27 - Vulnerabilities

Η εισαγωγή των εννοιών Common Vulnerabilities and Exposures (CVE) στην οντολογία μας έγινε με προγραμματιστική μέθοδο με την γλώσσα προγραμματισμού Python, λόγω του τεράστιου όγκου αυτών που έχουν καταγραφεί από το 1999 έως και σήμερα (324.617). Η πηγή αυτών που αντλήθηκαν σε csv αρχείο έγινε από την CVE® List του οργανισμού MITRE (Κέντρα Έρευνας και Ανάπτυξης). Η μορφή του περιεχομένου αυτού του αρχείου ήταν όπως φαίνεται:

```
CVE-2024-6303,Candidate,"Missing authorization in Client-Server API in Conduit <=0.7.0, allowing for
any alias to be removed and added to another room, which can be used for privilege escalation by
moving the #admins alias to a room which they control, allowing them to run commands resetting
passwords, siging json with the server's key, deactivating users, and more","MISC:https://conduit.rs/
changelog/#v0-8-0-2024-06-12 | URL:https://conduit.rs/changelog/#v0-8-0-2024-06-12 |
MISC:https://gitlab.com/famedly/conduit/-/releases/v0.8.0 | URL:https://gitlab.com/famedly/conduit/
-/releases/v0.8.0",Assigned (20240625),"None (candidate not yet proposed)",""
CVE-2024-6304,Candidate,"** RESERVED ** This candidate has been reserved by an organization or
individual that will use it when announcing a new security problem. When the candidate has been
publicized, the details for this candidate will be provided.","",Assigned (20240625),"None (candidate
not yet proposed)",""
CVE-2024-6305,Candidate,"WordPress Core is vulnerable to Stored Cross-Site Scripting via the Template
Part Block in various versions up to 6.5.5 due to insufficient input sanitization and output escaping
on the 'tagName' attributes. This makes it possible for authenticated attackers, with
contributor-level access and above, to inject arbitrary web scripts in pages that will execute
whenever a user accesses an injected page.","MISC:https://core.trac.wordpress.org/changeset/
58471 | URL:https://core.trac.wordpress.org/changeset/58471 | MISC:https://wordpress.org/news/
2024/06/wordpress-6-5-5/ | URL:https://wordpress.org/news/2024/06/wordpress-6-5-5/ |
MISC:https://www.wordfence.com/threat-intel/vulnerabilities/id/2a225ccb-a7dc-4437-bd97-b309d6ae6a47?
source=cve | URL:https://www.wordfence.com/threat-intel/vulnerabilities/id/
2a225ccb-a7dc-4437-bd97-b309d6ae6a47?source=cve",Assigned (20240625),"None (candidate not yet proposed)
",""
```

Εικόνα 28 - Μορφή αρχείου CVEs

Ο κώδικας python που χρησιμοποιήθηκε για την μετατροπή σε μορφή Turtle, θα υπάρχει ολόκληρος στο Παράρτημα Α στο τέλος αυτού του εγγράφου. Κάτω βλέπουμε και απόσπασμα του κώδικα που χρησιμοποιήθηκε:

```python
import pandas as pd
from rdflib import Graph, Namespace, RDF, OWL, SKOS, Literal, URIRef

# File path
csv_file = "/Users/paschalesmpekas/Downloads/allitems.csv"

# Read CSV while skipping metadata
df = pd.read_csv(csv_file, skiprows=8, encoding="ISO-8859-1", dtype=str, low_memory=False)

# Rename columns for clarity
df.columns = ["CVE_ID", "Status", "Description", "References", "Phase", "Votes", "Comments"]

# Drop empty or irrelevant rows
df.dropna(subset=["CVE_ID", "Description"], inplace=True)

# Define OWL Graph
g = Graph()

# Define namespaces
BASE_URI = "http://www.semanticweb.org/paschalesmpekas/ontologies/2024/9/CTI.skos#"
EX = Namespace(BASE_URI)

g.bind("ex", EX)
g.bind("skos", SKOS)
g.bind("owl", OWL)

# Create the main CVE concept
cve_concept = URIRef(EX.CVE)
g.add((cve_concept, RDF.type, SKOS.Concept))
g.add((cve_concept, SKOS.prefLabel, Literal("Common Vulnerabilities and Exposures", lang="en")))

# Define Cybersecurity Glossary Concept Scheme
glossary_scheme = URIRef(EX.CYBERSECURITY_GLOSSARY)
g.add((glossary_scheme, RDF.type, SKOS.ConceptScheme))
g.add((glossary_scheme, SKOS.prefLabel, Literal("Cybersecurity Glossary", lang="en")))

# Process each CVE entry
for _, row in df.iterrows():
    cve_id = row["CVE_ID"].strip()
    description = row["Description"].strip()

    cve_uri = URIRef(EX + cve_id)

    # Define CVE as Named Individual & SKOS Concept
    g.add((cve_uri, RDF.type, OWL.NamedIndividual))
    g.add((cve_uri, RDF.type, SKOS.Concept))

    # Link CVE to broader category and glossary scheme
    g.add((cve_uri, SKOS.broader, cve_concept))
    g.add((cve_uri, SKOS.inScheme, glossary_scheme))

    # Add CVE details
    g.add((cve_uri, SKOS.prefLabel, Literal(cve_id, lang="en")))
    g.add((cve_uri, SKOS.definition, Literal(description, lang="en")))

# Save as OWL (Turtle format)
owl_file = "cve_ontology.ttl"
g.serialize(destination=owl_file, format="turtle")

print(f"OWL file '{owl_file}' created successfully!")
```

Εικόνα 29 - Script μετατροπής σε μορφή Turtle

Φτάνοντας στην τελική μορφή όπου επιθυμούσαμε του προηγούμενου δείγματος, όπως:

```
###  http://www.semanticweb.org/paschalesmpekas/ontologies/2024/9/CTI.skos/CVE-2024-6303
:CVE-2024-6303 rdf:type owl:NamedIndividual ,
                        skos:Concept ;
               skos:broader :CVE ;
               skos:inScheme :CYBERSECURITY_GLOSSARY ;
               skos:definition "Missing authorization in Client-Server API in Conduit <=0.7.0, allowing for any alias to be removed and added to another room, which can be used for privilege
               escalation by moving the #admins alias to a room which they control, allowing them to run commands resetting passwords, siging json with the server's key, deactivating users, and
               more"@en ;
               skos:prefLabel "CVE-2024-6303"@en .


###  http://www.semanticweb.org/paschalesmpekas/ontologies/2024/9/CTI.skos/CVE-2024-6304
:CVE-2024-6304 rdf:type owl:NamedIndividual ,
                        skos:Concept ;
               skos:broader :CVE ;
               skos:inScheme :CYBERSECURITY_GLOSSARY ;
               skos:definition "** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been
               publicized, the details for this candidate will be provided."@en ;
               skos:prefLabel "CVE-2024-6304"@en .


###  http://www.semanticweb.org/paschalesmpekas/ontologies/2024/9/CTI.skos/CVE-2024-6305
:CVE-2024-6305 rdf:type owl:NamedIndividual ,
                        skos:Concept ;
               skos:broader :CVE ;
               skos:inScheme :CYBERSECURITY_GLOSSARY ;
               skos:definition "WordPress Core is vulnerable to Stored Cross-Site Scripting via the Template Part Block in various versions up to 6.5.5 due to insufficient input sanitization and
               output escaping on the 'tagName' attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that
               will execute whenever a user accesses an injected page."@en ;
               skos:prefLabel "CVE-2024-6305"@en .
```

Εικόνα 30 - Μορφή Turtle των CVEs

Στο πλαίσιο της κυβερνοασφάλειας, η αναγνώριση και η αξιολόγηση των ευπαθειών σε ένα σύστημα αποτελεί κρίσιμο βήμα για την ανάλυση κινδύνων και την γρήγορη λήψη αποφάσεων στο θέμα της ασφαλείας. Για το σκοπό αυτό, χρησιμοποιείται το CVSS (Common Vulnerability Scoring System), το οποίο αναφέρετε ως ένα τυποποιημένο σύστημα βαθμολόγησης των ευπαθειών και παρέχει μια αντικειμενική μέθοδο αξιολόγησης της ευπάθειας (FIST, 2015).

Το CVSS αναπτύχθηκε από το Forum of Incident Response and Security Teams (FIRST) και είναι ένα διεθνώς αναγνωρισμένο πρότυπο αξιολόγησης. Αποτελείται από έναν αριθμητικό δείκτη (score) από το 0 έως το 10 και συνοδεύεται από κατηγορίες σοβαρότητας της κατάστασης όπως: Low, Medium, High, Critical.

Η τρέχουσα έκδοση (CVSS v4.0) λαμβάνει υπόψη πολλαπλές μεταβλητές, όπως:

- Τον τρόπο πρόσβασης του επιτιθέμενου.
- Δυσκολία μιας επίθεσης.
- Αντίκτυπο σε εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα,
- Την ανάγκη για ανθρώπινη αλληλεπίδραση,
- Τυχόν άλλα απαιτούμενα προνόμια.

Ο παρακάτω πίνακας συνοψίζει την βαθμολόγηση και τις αντίστοιχες κατηγορίες σοβαρότητας, σύμφωνα με το πρότυπο CVSS v4.0. Αποτελεί ένα χρήσιμο εργαλείο για τους ανθρώπους σε θέματα ασφάλειας συστημάτων, ώστε να κατηγοριοποιούν τις απειλές και να παίρνουν άμεσα μέτρα ενίσχυσης της άμυνας.

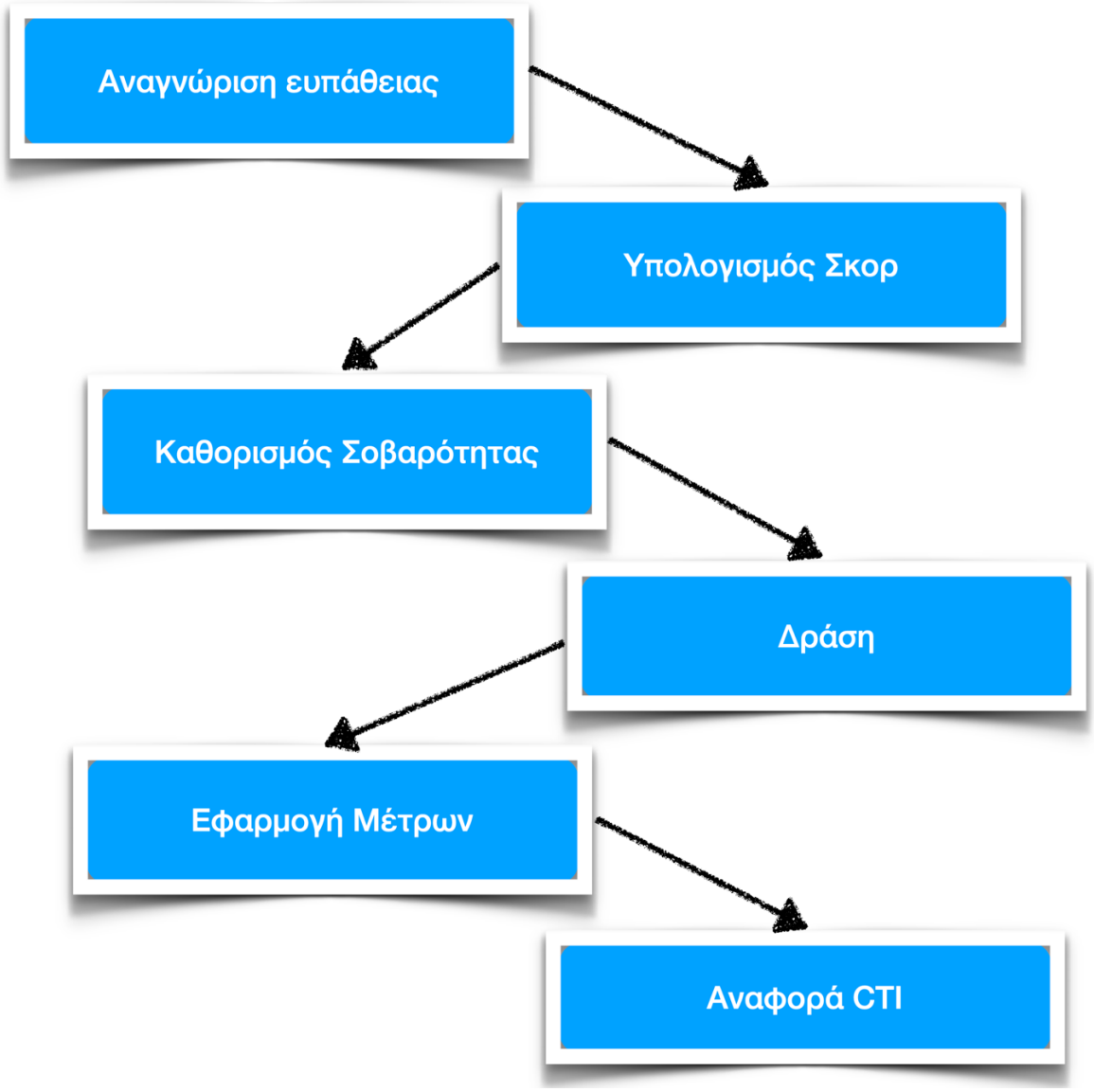
Πίνακας 6 - CVSS

Βαθμολογία (0 – 10)	***Σοβαρότητα***	***Περιγραφή***
0.0	None (Καμία)	Δεν υπάρχει πραγματική απειλή ή κίνδυνος.
0.1 – 3.9	Low (Χαμηλή)	Χαμηλής σοβαρότητας κίνδυνοι, δύσκολα εκμεταλλεύσιμες.
4.0 – 6.9	Medium (Μεσαία)	Μέτριου επιπέδου κίνδυνοι, μπορεί να προκαλέσουν προβλήματα.
7.0 – 8.9	High (Υψηλή)	Σοβαρές ευπάθειες που μπορούν να προκαλέσουν σημαντική ζημιά ή αναστολή των υπηρεσιών.
9.0 – 10.0	Critical (Κρίσιμη)	Ευπάθειες που αν δεν αντιμετωπιστούν άμεσα μπορεί να οδηγήσουν σε πλήρη παραβίαση ή καταστροφή συστημάτων.

Πότε χρησιμοποιούμε το CVSS Score στο Cyber Threat Intelligence (CTI);

- Όταν αξιολογούμε τη σοβαρότητα μιας νέας ευπάθειας που έχει εντοπιστεί ή δημοσιευτεί στο λεξικό του CVE.
- Κατά την κατηγοριοποίηση των ενεργειών απόκρισης όπως τα υψηλά CVSS Scores δείχνουν ότι πρέπει να δράσουμε άμεσα.
- Στη δημιουργία αναφορών CTI και για την ανάλογη ιεραρχική προώθηση του προς άλλα τμήματα ενός οργανισμού (όπως IT, Risk Management).
- Όταν αποφασίζουμε ποια patches ή ποιες ενημερώσεις πρέπει να εγκατασταθούν στο συστήματά μας.
- Στη συσχέτιση των πληροφοριών των απειλών, συνδυάζοντας ευπάθειες με γνωστά Indicators of Compromise (IoCs).

Μπορούμε να δούμε και τα βήματα που ακολουθούνται σε ένα περιστατικό επίθεσης στο σύστημα από την στιγμή της αναγνώρισης έως το τελικό στάδιο που είναι η αναφορά στο παρακάτω διάγραμμα ροής:



Εικόνα 31 - Διάγραμμα ροής Βημάτων CVSS

4.4 Ανάλυση Οντολογίας

Για την κατανόηση της δομής της οντολογίας που υλοποιήθηκε, πραγματοποιήθηκε εξαγωγή και στατιστική ανάλυση των δομικών στοιχείων της μέσω των εργαλείων Protégé ontology metrics και Python. Η οπτικοποίηση των στατιστικών δεδομένων πραγματοποιήθηκε με χρήση γραφημάτων, τα οποία παρέχουν μια ξεκάθαρη εικόνα για την δομή και την θέση των εννοιών, των ιδιοτήτων και των σχέσεών τους. Αναλύθηκαν ο αριθμός των κλάσεων των individuals των ιδιοτήτων και οι κύριοι τύποι αξιωμάτων που χαρακτηρίζουν την οντολογία. Μέσα από τα διαγράμματα, αναδεικνύονται η ένταση στη χρήση των instances, η απλότητα ή η πολυπλοκότητα της δομής, η οργάνωση των σχέσεων και η χρήση των annotations.
Τα παρακάτω γραφήματα με την βοήθεια της python (ο κώδικας στο ΠΑΡΑΡΤΗΜΑ Β) δίνουν μια λεπτομερή εικόνα της οντολογίας σε αριθμούς, επιτρέποντας την αναγνώριση βασικών χαρακτηριστικών που αναπαρίσταται και αξιοποιείται η γνώση στον τομέα του Cyber Threat Intelligence.

Από Ontology Metrics του protégé, αντλήσαμε τους στατιστικούς αριθμούς όπως:

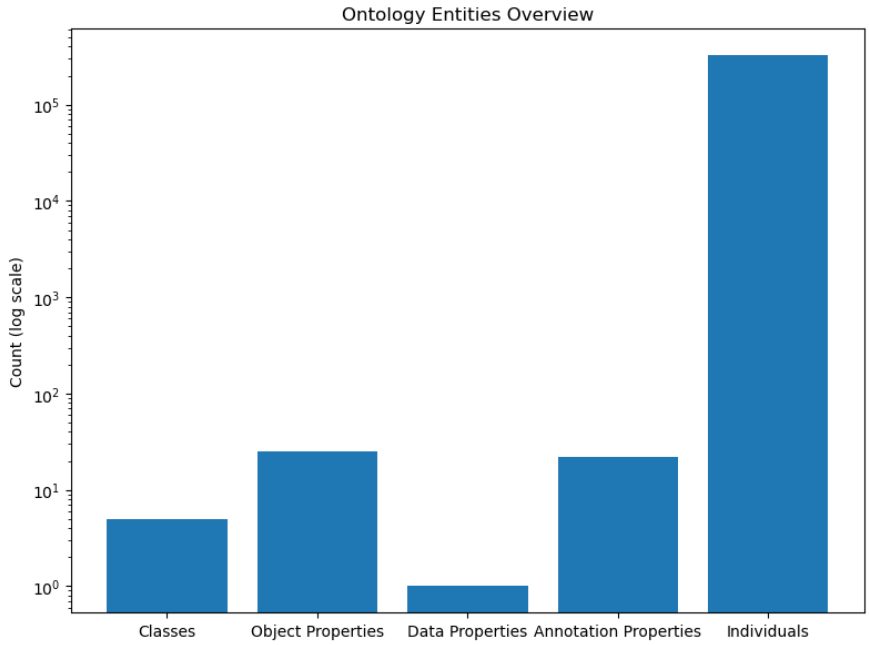
Ontology metrics:

Axiom	1.952.280
Logical axiom count	976.279
Declaration axioms count	325.345
Class count	5
Object property count	25
Data property count	1
Individual count	325.302
Annotation Property count	22
Class axioms	
SubClassOf	1
EquivalentClasses	0
DisjointClasses	3
GCI count	0
Hidden GCI Count	0
Object property axioms	
SubObjectPropertyOf	17
EquivalentObjectProperties	0
InverseObjectProperties	4
DisjointObjectProperties	0
FunctionalObjectProperty	1
InverseFunctionalObjectProperty	0
TransitiveObjectProperty	4
SymmetricObjectProperty	5
AsymmetricObjectProperty	0
ReflexiveObjectProperty	0
IrrefexiveObjectProperty	0
ObjectPropertyDomain	5
ObjectPropertyRange	6
SubPropertyChainOf	0

Data property axioms	
SubDataPropertyOf	0
EquivalentDataProperties	0
DisjointDataProperties	0
FunctionalDataProperty	0
DataPropertyDomain	0
DataPropertyRange	0
Individual axioms	
ClassAssertion	325.097
ObjectPropertyAssertion	651.136
DataPropertyAssertion	0
NegativeObjectPropertyAssertion	0
NegativeDataPropertyAssertion	0
SameIndividual	0
DifferentIndividuals	0
Annotation axioms	
AnnotationAssertion	650.625
AnnotationPropertyDomain	0
AnnotationPropertyRangeOf	0

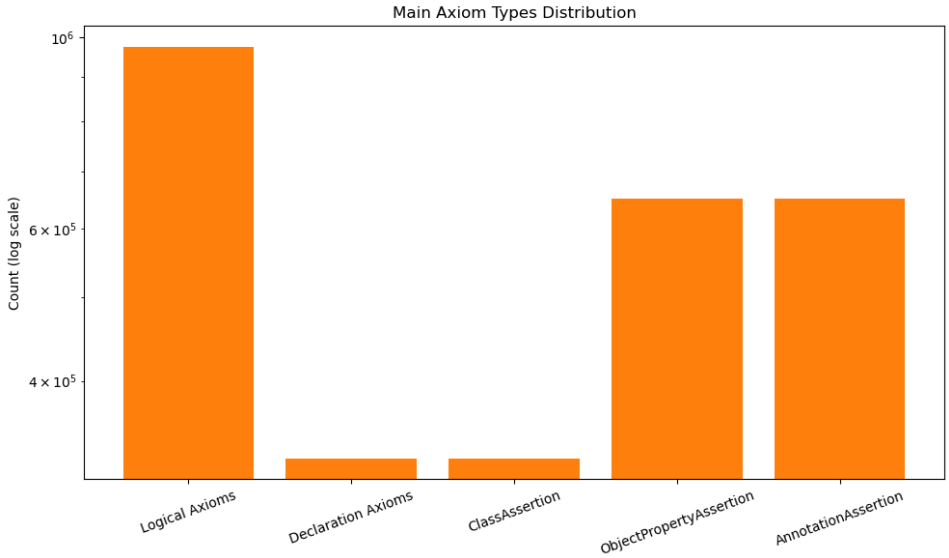
Εικόνα 32 - Ontology Metrics

Και με την βοήθεια της Python και των βιβλιοθηκών που την απαρτίζουν για την εξαγωγή γραφημάτων όπως η matplotlib, εξαγάγαμε τα γραφήματα με την σειρά όπως την παραπάνω εικόνα:



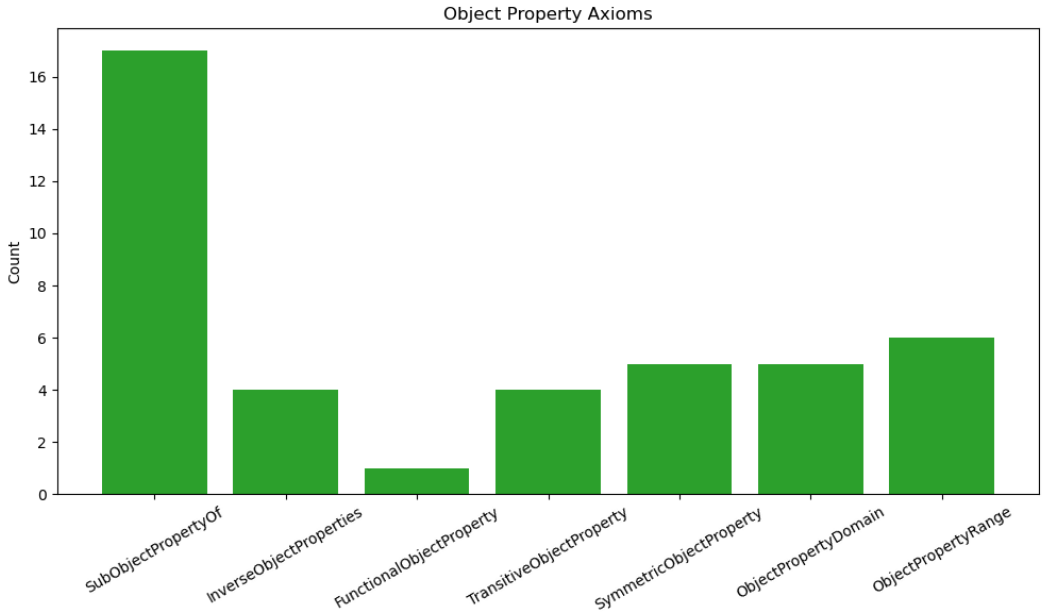
Εικόνα 33 - Ontology Entities Overview

Το παραπάνω γράφημα παρουσιάζει τη γενική εικόνα της οντολογίας. Παρατηρείται ότι ο αριθμός των εννοιών (individuals) υπερβαίνει κατά πολύ τον αριθμό των κλάσεων και των ιδιοτήτων. Αυτό αποδεικνύει πως η οντολογία έχει επικεντρωθεί στην αναπαράσταση μεγάλου όγκου δεδομένων (instances), με απλή και περιορισμένη ταξινομική δομή (μόλις 5 κλάσεις) λόγο του SKOS μοντέλου που χρησιμοποιήσαμε για την δημιουργία της.



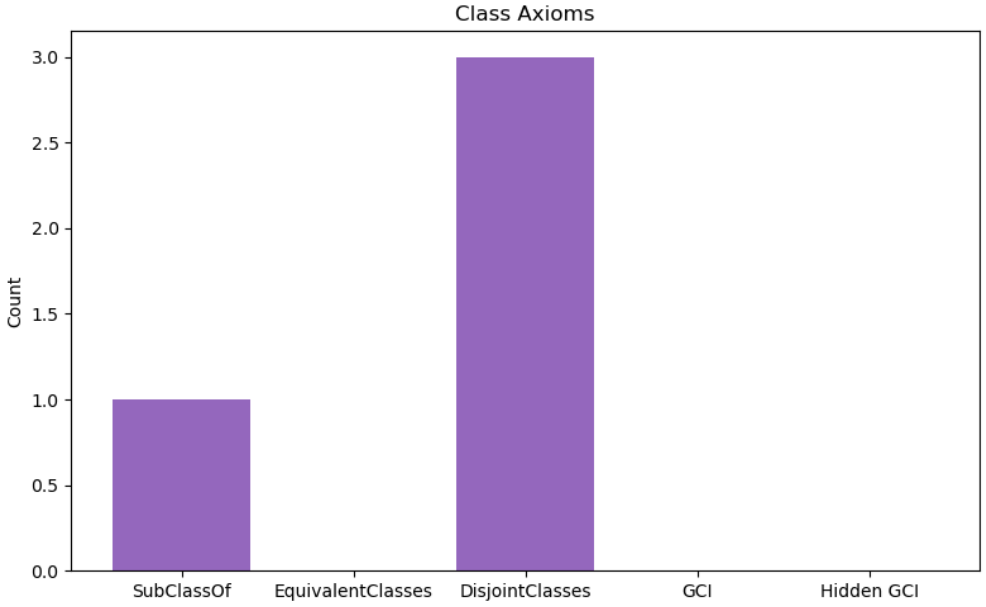
Εικόνα 34 - Main Axiom Types

Το δεύτερο γράφημα δείχνει την κατανομή των βασικών τύπων αξιωμάτων στην οντολογία. Τα assertions που σχετίζονται με Class Assertion, Object Property Assertion, Annotation Assertion, είναι πολύ περισσότερα από τα declaration axioms. Αυτό αποδεικνύει τη λειτουργικότητα της οντολογίας για καταγραφή πληροφοριών και σχέσεων μεταξύ συγκεκριμένων entities.



Εικόνα 35 - Object Property Axioms

Η χρήση των annotation assertions φαίνεται καθαρά σε αυτό το γράφημα. Αυτό υποδηλώνει ότι η οντολογία βασίζεται σημαντικά σε annotations για την παροχή πρόσθετων πληροφοριών και metadata, όπως περιγραφές, συσχετισμούς με εξωτερικές πηγές (άλλες SKOS ή μη οντολογίες). Συνοψίζοντας, τα στατιστικά δείχνουν ένα μοντέλο κυρίως για την αναπαράσταση μεγάλου όγκου δεδομένων, με έμφαση στα individuals και τις σχέσεις τους με μικρή πολυπλοκότητα σε classes και properties. Αυτό αποδεικνύει πως μια τέτοια οντολογία είναι ιδανική για χώρους υλοποίησης όπως το Cyber Threat Intelligence, όπου η ανάγκη για αποθήκευση και ανάλυση πολλών εννοιών και συσχετίσεων είναι μεγάλη και απαραίτητη.

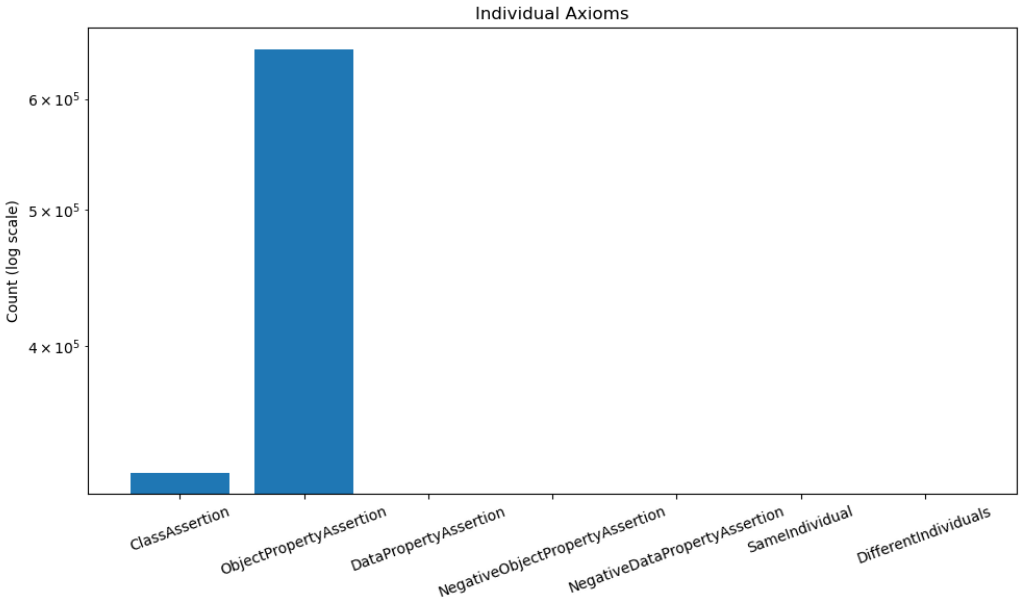


Εικόνα 36 - Class Axioms

Η ιεραρχία και η πολυπλοκότητα στις κλάσεις της οντολογίας είναι σχεδόν ανύπαρκτη, όπως φαίνεται από το αανωτέρω γράφημα. Υπάρχει μόνο ένα SubClassOf και ελάχιστες DisjointClasses, ενώ οι υπόλοιποι τύποι αξιωμάτων δεν υπάρχουν καθόλου. Αυτό αποτυπώνει ότι η οντολογία δεν χρησιμοποιεί ένα σύνθετο εννοιολογικό μοντέλο, αλλά εστιάζει κυρίως σε επίπεδο instances, σε αυτό όπως προ είπαμε οφείλεται στην επιλογή του SKOS μοντέλου.

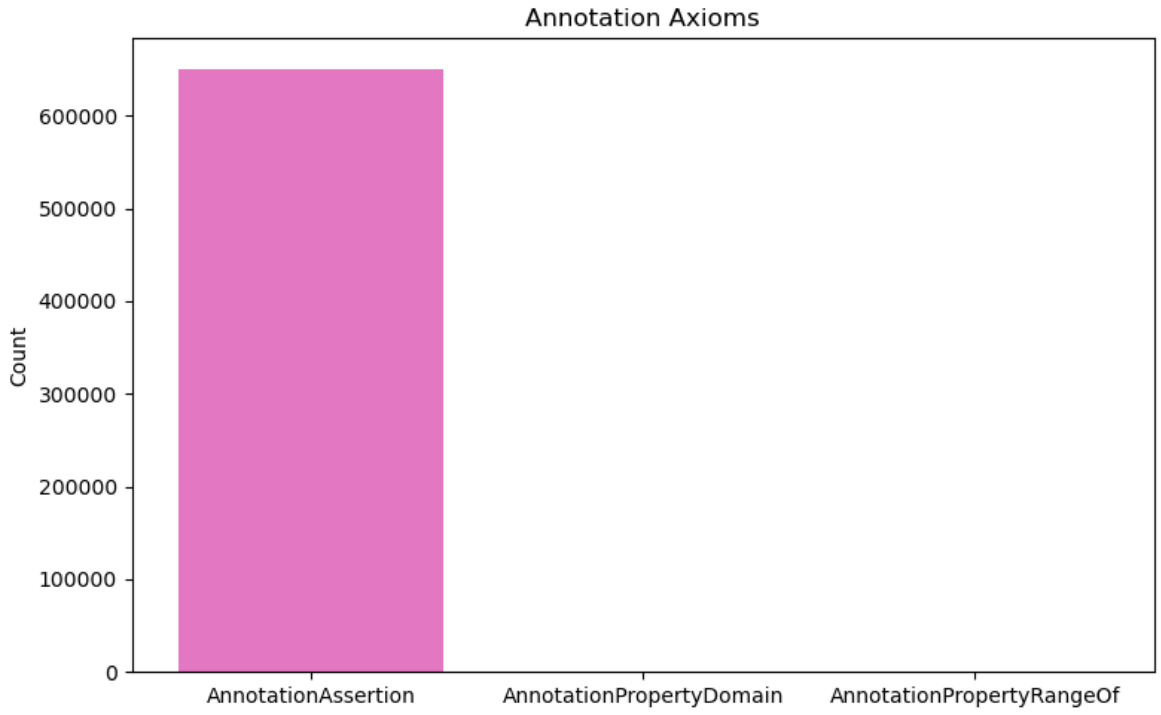
Εικόνα 37 - Data property Axioms

Όπως προ είπαμε με την επιλογή του μοντέλου SKOS παρατηρούμε στο ανωτέρω γράφημα την πλήρη απουσία των Data properties. Αυτό σημαίνει ότι η αναπαράσταση των δεδομένων γίνεται σχεδόν αποκλειστικά μέσω Object Properties και annotations και όχι με απευθείας αποθήκευση τιμών δεδομένων.



Εικόνα 38 - Individual Axioms

Τα assertions για τα individuals ως έννοιες αποτελούν τον κεντρικό πυρήνα της οντολογίας. Οι μοναδικές κατηγορίες είναι οι ClassAssertion και ObjectPropertyAssertion, που αντιστοιχούν στην ταξινόμηση των individuals σε κλάσεις και στον καθορισμό των σχέσεων μεταξύ τους.



Εικόνα 39 - Annotations Axioms

Η πλήρη χρήση των AnnotationAssertion φαίνεται ξεκάθαρα από το ανωτέρω γράφημα. Αυτό υποδηλώνει ότι η οντολογία βασίζεται σημαντικά σε annotations για την επιπρόσθετη παροχή πληροφοριών και metadata, όπως περιγραφές, συσχετίσεις μεταξύ εννοιών με εξωτερικές πηγές (άλλες οντολογίες κ.α.). Να υπενθυμίσουμε πως ο τεράστιος αριθμός που βλέπουμε στο γράφημά μας, οφείλεται στον τεράστιο αριθμό CVEs που συμπεριλάβαμε στην οντολογία μας στην ως υποκατηγορία της έννοιας Vulnerabilities.

Συνοψίζοντας, τα στατιστικά της οντολογίας αναδεικνύουν ένα μοντέλο SKOS κυρίως για την αναπαράσταση μεγάλων όγκων δεδομένων, με έμφαση στα individuals και τις σχέσεις τους, και με ελάχιστη πολυπλοκότητα σε επίπεδο κλάσεων. Μια τέτοια οντολογία είναι ιδανική για περιβάλλοντα όπως το Cyber Threat Intelligence, όπου η ανάγκη για αποθήκευση και ανάλυση πολλών οντοτήτων-εννοιών και συσχετίσεων είναι πολύ μεγάλη.

Κεφάλαιο 5ο: Συμπεράσματα και προτάσεις βελτίωσης

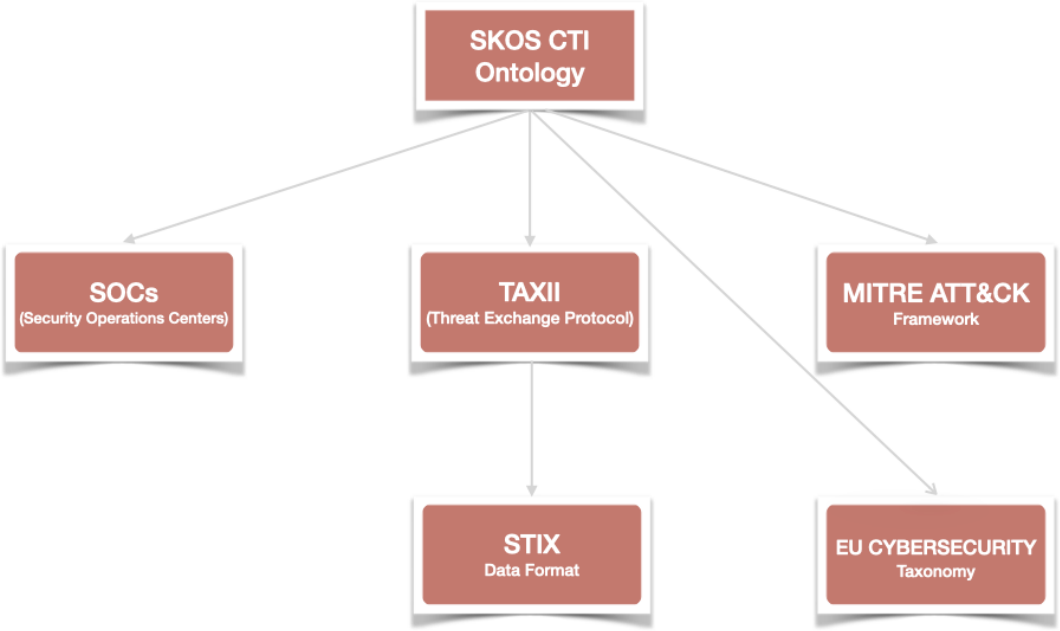
Η παρούσα διπλωματική εργασία ανέδειξε τη χρησιμότητα του μοντέλου SKOS για την ανάπτυξη μιας δομημένης, επεκτάσιμης και συμβατής οντολογίας στον χώρο του Cyber Threat Intelligence (CTI) και του Σημασιολογικού Ιστού. Μέσα από αυτό το μοντέλο, δημιουργήθηκε ένα λεξιλόγιο εννοιών και σχέσεων που καλύπτει βασικούς άξονες και όχι μόνο των κυβερνοαπειλών όπως: η ταυτότητα ενός επιτιθέμενου, οι στόχοι που έχουν, οι τεχνικές που χρησιμοποιούν, τους δείκτες παραβίασης και τις υπάρχουσες ευπάθειες.
Η προσέγγιση αυτή πέτυχε:

- Την απλοποίηση μοντελοποίησης των εννοιών με χρήση SKOS ιδιοτήτων.
- Τη δυνατότητα χρήσης της οντολογίας από πολλούς και διάφορους οργανισμούς ή μη, με κοινό υπόβαθρο στο θέμα πληροφορίας.
- Τη διασύνδεση με πραγματικά δεδομένα CTI, όπως τεχνικές επιθέσεων, IoCs και TTPs κ.α.

Προτάσεις για μελλοντική βελτίωση:

1. Διαλειτουργικότητα με Λειτουργικά Κέντρα Ασφαλείας (SOCs). Η οντολογία μπορεί να χρησιμοποιηθεί ως κοινό λεξιλόγιο ανάμεσα σε SOCs διαφορετικών οργανισμών. Μέσω της χρήσης SKOS ιδιοτήτων και RDF, οι πληροφορίες μπορούν να ανταλλάσσονται ή να αναλύονται σε κοινό πλαίσιο, μειώνοντας τις ασάφειες και αυξάνοντας την αποτελεσματικότητα.
2. Διασύνδεση με πρότυπα όπως STIX και MITRE ATT&CK. Μελλοντικά, η οντολογία μπορεί να επεκταθεί με μηχανισμούς mapping σε άλλα υπάρχοντα πρότυπα όπως:
    - Το STIX 2.1 για την αναπαράσταση IoCs, Threat Actors και TTPs σε μηχανική μορφή.
    - Το MITRE ATT&CK με χρήση των τεχνικών και τακτικών ως concepts με ιδιότητες skos:exactMatch ή skos:closeMatch.

    Αυτό θα επιτρέψει τη συγχώνευση δεδομένων από πολλές και διάφορες πηγές διατηρώντας τη συνοχή τους σημασιολογικά.
3. Διασύνδεση με την Cybersecurity Taxonomy της Ευρωπαϊκής Ένωσης. Η υιοθέτηση της επίσημης οντολογίας κυβερνοασφάλειας της Ε.Ε. αποτελεί υπερισχύουσα προτεραιότητα. Η μελλοντική διασύνδεση με αυτή την οντολογία θα:
    - Διευκολύνει τη συνεργασία με φορείς του δημόσιου και ιδιωτικού τομέα σε ευρωπαϊκό επίπεδο.
    - Επιτρέψει αυτόματη αντιστοίχιση των όρων, των εννοιών καθώς και επαναχρησιμοποίηση ταξινομιών.
4. Επέκταση OWL restrictions στο μέλλον μπορεί να ενισχύσει τη δυνατότητα της «λογικής» και της εξαγωγής συμπερασμάτων και πολύπλοκων ερωτημάτων με SPARQL.
5. Οπτικοποίηση και ενσωμάτωση σε πλατφόρμες Threat Intelligence Platforms (TIP). Προτείνεται η δημιουργία εργαλείων οπτικοποίησης όπως το plugin OntoGraf που χρησιμοποιήσαμε ή web based SPARQL Dashboards για την αναζήτηση εντός οντολογίας καθώς και η ενσωμάτωση της οντολογίας σε TIPs, για την ανάλυση και την ενημέρωσή τους.



Εικόνα 40 - Διασύνδεση SKOS CTI Ontology με Πρότυπα και Πλατφόρμες

Το παραπάνω διάγραμμα απεικονίζει πώς η οντολογία μας για το Cyber Threat Intelligence μπορεί μελλοντικά να ενσωματωθεί και να συνεργαστεί με διεθνή πρότυπα και επιχειρησιακές υποδομές.

Τελικώς η εργασία αυτή βάζει τις βάσεις για τη δημιουργία μιας πλούσιας με διαλειτουργικότητα οντολογίας στο Cyber Threat Intelligence, ικανής να υποστηρίξει την ανταλλαγή και ανάλυση πληροφοριών μεταξύ οργανισμών και όχι μόνο καθώς και συστημάτων. Με την κατάλληλη επέκταση, βελτίωση και σύνδεση με διεθνή πρότυπα, το σύστημα αυτό μπορεί να αποτελέσει ένα πυλώνα για την ευφυία των απειλών στον κυβερνοχώρο.

ΠΑΡΑΡΤΗΜΑ Α : Script Python για την εξαγωγή των CVEs

```
import pandas as pd
from rdflib import Graph, Namespace, RDF, OWL, SKOS, Literal, URIRef

# File path
csv_file = "/Users/paschalesmpekas/Downloads/allitems.csv"

# Read CSV while skipping metadata
df = pd.read_csv(csv_file, skiprows=8, encoding="ISO-8859-1", dtype=str, low_memory=False)

# Rename columns for clarity
df.columns = ["CVE_ID", "Status", "Description", "References", "Phase", "Votes", "Comments"]

# Drop empty or irrelevant rows
df.dropna(subset=["CVE_ID", "Description"], inplace=True)

# Define OWL Graph
g = Graph()

# Define namespaces
BASE_URI = "http://www.semanticweb.org/paschalesmpekas/ontologies/2024/9/CTI.skos#"
EX = Namespace(BASE_URI)

g.bind("ex", EX)
g.bind("skos", SKOS)
g.bind("owl", OWL)

# Create the main CVE concept
cve_concept = URIRef(EX.CVE)
g.add((cve_concept, RDF.type, SKOS.Concept))
g.add((cve_concept, SKOS.prefLabel, Literal("Common Vulnerabilities and Exposures", lang="en")))

# Define Cybersecurity Glossary Concept Scheme
glossary_scheme = URIRef(EX.CYBERSECURITY_GLOSSARY)
g.add((glossary_scheme, RDF.type, SKOS.ConceptScheme))
g.add((glossary_scheme, SKOS.prefLabel, Literal("Cybersecurity Glossary", lang="en")))

# Process each CVE entry
for _, row in df.iterrows():
    cve_id = row["CVE_ID"].strip()
    description = row["Description"].strip()

    cve_uri = URIRef(EX + cve_id)

    # Define CVE as Named Individual & SKOS Concept
    g.add((cve_uri, RDF.type, OWL.NamedIndividual))
    g.add((cve_uri, RDF.type, SKOS.Concept))

    # Link CVE to broader category and glossary scheme
    g.add((cve_uri, SKOS.broader, cve_concept))
    g.add((cve_uri, SKOS.inScheme, glossary_scheme))

    # Add CVE details
    g.add((cve_uri, SKOS.prefLabel, Literal(cve_id, lang="en")))
    g.add((cve_uri, SKOS.definition, Literal(description, lang="en")))

# Save as OWL (Turtle format)
owl_file = "cve_ontology.ttl"
g.serialize(destination=owl_file, format="turtle")

print(f"OWL file '{owl_file}' created successfully!")
```

ΠΑΡΑΡΤΗΜΑ Β: Script Python για την εξαγωγή γραφημάτων

```
import matplotlib.pyplot as plt

# 1. Overview of ontology entities (Classes, Properties, Individuals)
entities_labels = ['Classes', 'Object Properties', 'Data Properties', 'Annotation Properties',
'Individuals']
entities_counts = [5, 25, 1, 22, 325302]

plt.figure(figsize=(8,6))
plt.bar(entities_labels, entities_counts)
plt.yscale('log')
plt.title('Ontology Entities Overview')
plt.ylabel('Count (log scale)')
plt.tight_layout()
plt.show()

# 2. Distribution of main axiom types
axiom_labels = ['Logical Axioms', 'Declaration Axioms', 'ClassAssertion', 'ObjectPropertyAssertion',
'AnnotationAssertion']
axiom_counts = [976279, 325345, 325097, 651136, 650625]

plt.figure(figsize=(10,6))
plt.bar(axiom_labels, axiom_counts, color="tab:orange")
plt.yscale('log')
plt.title('Main Axiom Types Distribution')
plt.ylabel('Count (log scale)')
plt.xticks(rotation=20)
plt.tight_layout()
plt.show()

# 3. Object Property Axioms details
obj_prop_labels = [
    'SubObjectPropertyOf', 'InverseObjectProperties', 'FunctionalObjectProperty',
    'TransitiveObjectProperty', 'SymmetricObjectProperty', 'ObjectPropertyDomain',
    'ObjectPropertyRange'
]
obj_prop_counts = [17, 4, 1, 4, 5, 5, 6]

plt.figure(figsize=(10,6))
plt.bar(obj_prop_labels, obj_prop_counts, color="tab:green")
plt.title('Object Property Axioms')
plt.ylabel('Count')
plt.xticks(rotation=30)
plt.tight_layout()
plt.show()

# 4. Class Axioms
class_axioms_labels = ['SubClassOf', 'EquivalentClasses', 'DisjointClasses', 'GCI', 'Hidden GCI']
class_axioms_counts = [1, 0, 3, 0, 0]

plt.figure(figsize=(8,5))
plt.bar(class_axioms_labels, class_axioms_counts, color="tab:purple")
plt.title('Class Axioms')
plt.ylabel('Count')
plt.tight_layout()
plt.show()

# 5. Data Property Axioms (all zero, shown for completeness)
data_prop_labels = [
    'SubDataPropertyOf', 'EquivalentDataProperties', 'DisjointDataProperties',
    'FunctionalDataProperty', 'DataPropertyDomain', 'DataPropertyRange'
]
data_prop_counts = [0, 0, 0, 0, 0, 0]

plt.figure(figsize=(12,5))
plt.bar(data_prop_labels, data_prop_counts, color="tab:gray")
plt.title('Data Property Axioms')
plt.ylabel('Count')
plt.tight_layout()
plt.show()
```

```
# 6. Individual Axioms
individual_axioms_labels = [
    'ClassAssertion', 'ObjectPropertyAssertion', 'DataPropertyAssertion',
    'NegativeObjectPropertyAssertion', 'NegativeDataPropertyAssertion',
    'SameIndividual', 'DifferentIndividuals'
]
individual_axioms_counts = [325097, 651136, 0, 0, 0, 0, 0]

plt.figure(figsize=(10,6))
plt.bar(individual_axioms_labels, individual_axioms_counts, color="tab:blue")
plt.yscale('log')
plt.title('Individual Axioms')
plt.ylabel('Count (log scale)')
plt.xticks(rotation=20)
plt.tight_layout()
plt.show()

# 7. Annotation Axioms
annotation_axioms_labels = [
    'AnnotationAssertion', 'AnnotationPropertyDomain', 'AnnotationPropertyRangeOf'
]
annotation_axioms_counts = [650625, 0, 0]

plt.figure(figsize=(8,5))
plt.bar(annotation_axioms_labels, annotation_axioms_counts, color="tab:pink")
plt.title('Annotation Axioms')
plt.ylabel('Count')
plt.tight_layout()
plt.show()
```

ΠΑΡΑΡΤΗΜΑ Γ: Οντολογία σε μορφή .ttl με τις κύριες έννοιες

```
@prefix : <http://www.semanticweb.org/paschalesmpekas/ontologies/2024/9/CTI.skos/> .
@prefix dc: <http://purl.org/dc/elements/1.1/>.
@prefix owl: <http://www.w3.org/2002/07/owl#>.
@prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>.
@prefix xml: <http://www.w3.org/XML/1998/namespace>.
@prefix xsd: <http://www.w3.org/2001/XMLSchema#>.
@prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#>.
@prefix skos: <http://www.w3.org/2004/02/skos/core#>.
@prefix skos1: <http://www.w3.org/2008/05/skos#>.
@prefix terms: <http://purl.org/dc/terms/>.
@base <http://www.semanticweb.org/paschalesmpekas/ontologies/2024/9/CTI.skos/>.

<http://www.semanticweb.org/paschalesmpekas/ontologies/2024/9/CTI.skos> rdf:type owl:Ontology ;
owl:imports <http://www.w3.org/2004/02/skos/core>;
terms:created "2021-04-26"^^xsd:date ;
terms:identifier "http://data.jrc.ec.europa.eu/ontology/cybersecurity/cybersecurity-taxonomy";
owl:versionInfo "25/03/2021";
skos:prefLabel "Cybersecurity taxonomy"@en;

<http://www.w3.org/2008/05/skos-xl#prefLabel>
<http://data.jrc.ec.europa.eu/ontology/cybersecurity/xl_en_6d00c842> .

#################################################################
#    Annotation properties
#################################################################

### http://purl.org/dc/terms/created
terms:created rdf:type owl:AnnotationProperty .

### http://purl.org/dc/terms/identifier
terms:identifier rdf:type owl:AnnotationProperty .

### http://www.w3.org/2004/02/skos/core#altLabel
Skos altLabel rdf:type owl:AnnotationProperty ;
              rdfs:subPropertyOf rdfs:label .

###  http://www.w3.org/2004/02/skos/core#definition
skos:definition rdf:type owl:AnnotationProperty ;
                rdfs:subPropertyOf rdfs:label .

### http://www.w3.org/2004/02/skos/core#example
skos:example rdf:type owl:AnnotationProperty ;
             rdfs:subPropertyOf rdfs:label .

###  http://www.w3.org/2004/02/skos/core#hiddenLabel
skos:hiddenLabel rdf:type owl:AnnotationProperty ;
                 rdfs:subPropertyOf rdfs:label .

### http://www.w3.org/2004/02/skos/core#historyNote
skos:historyNote rdf:type owl:AnnotationProperty ;
                 rdfs:subPropertyOf rdfs:label .

### http://www.w3.org/2004/02/skos/core#prefLabel
skos:prefLabel rdf:type owl:AnnotationProperty ;
               rdfs:subPropertyOf rdfs:label .

### http://www.w3.org/2004/02/skos/core#scopeNote
skos:scopeNote rdf:type owl:AnnotationProperty ;
               rdfs:subPropertyOf rdfs:label .

### http://www.w3.org/2008/05/skos-xl#prefLabel
<http://www.w3.org/2008/05/skos-xl#prefLabel> rdf:type owl:AnnotationProperty .

#################################################################
#    Datatypes
#################################################################

### http://www.w3.org/2001/XMLSchema#date
xsd:date rdf:type rdfs:Datatype .
```

```
#################################################################
#    Object Properties
#################################################################

###  http://www.w3.org/2004/02/skos/core#broader
skos:broader rdf:type owl:ObjectProperty .

###  http://www.w3.org/2004/02/skos/core#exactMatch
skos:exactMatch rdf:type owl:ObjectProperty .

### http://www.w3.org/2004/02/skos/core#inScheme
skos:inScheme rdf:type owl:ObjectProperty .

### http://www.w3.org/2004/02/skos/core#narrower
skos:narrower rdf:type owl:ObjectProperty .

### http://www.w3.org/2004/02/skos/core#related
skos:related rdf:type owl:ObjectProperty .

### http://www.w3.org/2004/02/skos/core#relatedMatch
skos:relatedMatch rdf:type owl:ObjectProperty .

### http://www.w3.org/2008/05/skos#hasTopConcept
skos1:hasTopConcept rdf:type owl:ObjectProperty .

### http://www.w3.org/2008/05/skos#narrower
skos1:narrower rdf:type owl:ObjectProperty .

### http://www.w3.org/2008/05/skos#topConceptOf
skos1:topConceptOf rdf:type owl:ObjectProperty .

#################################################################
#    Classes
#################################################################

### http://www.semanticweb.org/paschalesmpekas/ontologies/2024/9/CTI.skos/CYBERSECURITY_GLOSSARY
:CYBERSECURITY_GLOSSARY rdf:type owl:NamedIndividual ,
skos:ConceptScheme ;
skos1:hasTopConcept:DL;
skos:altLabel "CYBERSECURITY VOCABULARY"@en;
skos:definition "A well compiled list of definitions and explanations for words, ideas, and technology
frequently used in cybersecurity is called a cybersecurity glossary. Professionals, students, and anybody
else interested in cybersecurity will find this glossary helpful since it clarifies important terms and
jargon."@en;
skos:example "A well-organized glossary can simplify the complex language of cybersecurity, making the
field more accessible to those outside the industry while serving as a reference for professionals."@en
;
skos:prefLabel "CYBERSECURITY GLOSSARY"@en,
"Cybersecurity Glossary"@en.

### http://www.semanticweb.org/paschalesmpekas/ontologies/2024/9/CTI.skos/DL
:DL rdf:type owl:NamedIndividual ,
skos:Concept ;
skos:inScheme :CYBERSECURITY_GLOSSARY;
skos:relatedMatch <http://data.jrc.ec.europa.eu/ontology/cybersecurity/safety_security>;
skos1:topConceptOf:CYBERSECURITY_GLOSSARY;
skos:definition "Threat intelligence helps security teams be more proactive, enabling them to take
effective, data-driven actions to prevent cyberattacks before they occur. It can also help an organization
detect and respond to attacks in progress faster."@en;
skos:prefLabel "Cyber Threat Intelligence (CTI)"@en.

### http://www.w3.org/2004/02/skos/core#Concept
skos:Concept rdf:type owl:Class .

### http://www.w3.org/2004/02/skos/core#ConceptScheme
skos:ConceptScheme rdf:type owl:Class .

### http://www.semanticweb.org/paschalesmpekas/ontologies/2024/9/CTI.skos#Atomic_Indicators
:Atomic_Indicators rdf:type owl:NamedIndividual ,
skos:Concept;
skos:broader:DL;
skos:inScheme :CYBERSECURITY_GLOSSARY ;
skos:narrower :Email_Indicators ,
:Host-Based_Indicators ,
```

```
:Network_Indicators ;
skos:definition "Short-lived, low-level data points used to identify threats."@en;
skos:prefLabel "Atomic Indicators"@en .

###http://www.semanticweb.org/paschalesmpekas/ontologies/2024/9/CTI.skos/cybersecurity_tools_and_techni
ques
:cybersecurity_tools_and_techniques rdf:type owl:NamedIndividual ,
skos:Concept ;
skos:broader :DL ;
skos:inScheme :CYBERSECURITY_GLOSSARY ;
skos:narrower
<http://www.semanticweb.org/paschalesmpekas/ontologies/2024/9/CTI.skos#MITRE_ATT&CK_framework> ,
:BAS ,
:EDR ,
:FIM ,
:ISAC ,
:MAEC ,
:MISP ,
:MRTI ,
:OSINT ,
:Resilience ,
:SIEMs ,
:SOAR ,
:STIX ,
:TAXII ,
:TIPs ,
:YARA ,
:behavioral_analysis ,
:cybersecurity_maturity_model_certification ,
:data_encryption_at_rest ,
:data_loss_prevention ,
:digital_forensics ,
:endpoint_protection ,
:honeypot ,
:multi_factor_authentication ,
:network_access_control ,
:privileged_access_management ,
:sandbox ,
:secure_access_service_edge ,
:simulation_tools ,
:sinkholing ,
:zero_trust_architecture ;
skos:definition "Courses of Action refer to measures that can be taken to prevent or respond to
attacks."@en ;
skos:prefLabel "Courses  of  Action"@en .

### http://www.semanticweb.org/paschalesmpekas/ontologies/2024/9/CTI.skos/Threat_Actors
:Threat_Actors rdf:type owl:NamedIndividual ,
skos:Concept ;
skos:broader :DL ;
skos:inScheme :CYBERSECURITY_GLOSSARY ;
skos:narrower :Cyber_Fighters ,
:Cyber_Terrorists ,
:Cyber_criminals ,
:Hackers ,
:Hacktivists ,
:Insiders ,
:Nation_States ,
:Script_Kiddies ,
:Terrorists ;
skos:definition """Identity indicates an individual or a group of individuals that can manifest a threat.
• Internal
• External
– Capabilities + Intentions + Past Activities."""@en
skos:prefLabel "Identity"@en.

### http://www.semanticweb.org/paschalesmpekas/ontologies/2024/9/CTI.skos/Indicators_of_Compromise
:Indicators_of_Compromise rdf:type owl:NamedIndividual ,
skos:Concept ;
skos:broader:DL;
skos:inScheme :CYBERSECURITY_GLOSSARY ;
skos:narrower :Application_Specific_IoCs ,
:Behavioral_IoCs ,
:Email_Based_IoCs ,
```

```
:File_Based_IoCs ,
:Host-Based_IoCs ,
:Network_Based_IoCs ,
:Other_Advanced_IoCs ,
:Time_Based_IoCs ;
skos:definition "In cybersecurity, forensic data points known as Indicators of Compromise (IoCs) indicate
a possible or verified security breach in a system or network. Cybersecurity teams use these hints to
identify, look into, and address online dangers."@en ;
skos:example "Unusual network traffic patterns, malicious domain names, suspicious registry updates, IP
addresses, file hashes, and other artifacts left by attackers are examples of IoCs."@en ;
skos:prefLabel "Indicators of Compromise (IoCs)"@en ;
skos:scopeNote "Tracking IoCs is essential for identifying specific types of attacks (e.g., malware
infections, unauthorized access, data exfiltration) and for enhancing an organization's defense
mechanisms. By sharing and analyzing IoCs, security teams can better anticipate, prevent, and mitigate
cyber threats."@en .

###  http://www.semanticweb.org/paschalesmpekas/ontologies/2024/9/CTI.skos/Motivation
:Motivation rdf:type owl:NamedIndividual ,
skos:Concept ;
skos:broader :DL ;
skos:inScheme :CYBERSECURITY_GLOSSARY ;
skos:narrower
<http://www.semanticweb.org/paschalesmpekas/ontologies/2024/9/CTI.skos#Revenge/Punishment> ,
:Financial_Motivation ,
:Ideological_Motivation ,
:Military_Motivation ;
skos:definition "The driving force behind a threat actor's actions, often related to ideological,
military, financial, or personal objectives."@en ;
skos:prefLabel "Motivation"@en .

###  http://www.semanticweb.org/paschalesmpekas/ontologies/2024/9/CTI.skos/TTPs
:TTPs rdf:type owl:NamedIndividual ,
skos:Concept ;
skos:broader :DL ;
skos:inScheme :CYBERSECURITY_GLOSSARY ;
skos:narrower :Threat_Types ,
:procedures ,
:tactics ;
skos:altLabel "TTP"@en ;
skos:definition "TTPs refer to the patterns and methods attackers use. Tactics are high-level objectives
(e.g., gaining access), techniques are specific ways to achieve tactics (e.g., phishing), and procedures
are the technical details of execution. TTPs help cybersecurity teams anticipate attacker moves."@en ;
skos:prefLabel "Tactics, Techniques, and Procedures (TTPs)"@en .

###  http://www.semanticweb.org/paschalesmpekas/ontologies/2024/9/CTI.skos#Target
:Target rdf:type owl:NamedIndividual ,
skos:Concept ;
skos:broader :DL ;
skos:inScheme :CYBERSECURITY_GLOSSARY ;
skos:narrower :Companies ,
:Individuals ,
:Nations ,
:Organizations ,
:Sectors ;
skos:definition "The intended victim or affected entity of a cyberattack. Targets can include
organizations, companies, sectors, nations, and individuals."@en ;
skos:prefLabel "Target"@en .

###  http://www.semanticweb.org/paschalesmpekas/ontologies/2024/9/CTI.skos/Vulnerability
:Vulnerability rdf:type owl:NamedIndividual ,
skos:Concept ;
skos:broader :DL ;
skos:inScheme :CYBERSECURITY_GLOSSARY ;
skos:narrower :CVE ,
:CVSS ,
:Human_Vulnerabilities,
:Process_Vulnerabilities,
:System_Vulnerabilities;
skos:relatedMatch <http://data.jrc.ec.europa.eu/ontology/cybersecurity/vulnerability_analysis_response>
;
skos:definition "A vulnerability is a weakness which allows an attacker to compromise security (integrity,
confidentiality or availability)."@en;
skos:prefLabel "Vulnerabilities"@en.
```

ΒΙΒΛΙΟΓΡΑΦΙΑ

ATT&CK, M. (2015-2024). "ATT&CK." from https://attack.mitre.org.

Barnum, S. (2014). Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™).

Bechhofer, A. M. a. S. (2008). "SKOS Simple Knowledge Organization System RDF Schema." from https://www.w3.org/TR/2008/WD-skos-reference-20080829/skos.html.

Brickley, A. M. a. D. (2005). "SKOS Core Guide." from https://www.w3.org/2004/02/skos/core/guide/2005-10-06/.

Bromander, V. M. a. S. (2017). Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence. European Intelligence and Security Informatics.

Charalampos Bratsas, E. K. A., Alexandros K. Angelidis, and R. K. a. S. O. Lazaros Ioannidis (2024). "Knowledge Graphs and Semantic Web Tools in Cyber Threat Intelligence: A Systematic Literature Review." Cybersecurity and Privacy.

Eric M. Hutchins, M. J. C. a. R. M. A. (2011). Intelligence-Driven Computer Network Defense Informed byAnalysis ofAdversary Campaigns and Intrusion Kill Chains.

Eric W. Burger , M. D. G., Panos Kampanakis and Kevin A. Zhu (2014). Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies.

Flaborea, R. S. (2024). "The Cyber Kill Chain." from https://anticitizenone.medium.com/the-cyber-kill-chain-984358c79628.

FIST (2015). "Common Vulnerability Scoring System: Specification Document." from https://www.first.org/cvss/v4-0/specification-document.

Gilchrist, A. (2003). "Thesauri, taxonomies and ontologies – an etymological note." Emerald Insight **59**.

Grønberg, M. (2019). An Ontology for Cyber Threat Intelligence.

Guarino, N. (1998). Formal Ontology and Information Systems**:** 13.

Holland, M.-V. L. a. J. (2010). Guidelines for mapping into SKOS, dealing with translations.

Josang, V. M. a. A. (2018). Data-Driven Threat Hunting Using Sysmon. International Conference on Cryptography, Security and Privacy. Guiyang, China**:** 7.

Juan-Antonio Pastor-Sanchez, F. J. M. M. a. J. V. R.-M. (2009). Advantages of thesaurus representation using the Simple Knowledge Organization System (SKOS) compared with proposed alternatives **14:** 16.

Kourie, V. P. a. D. G. (2014). "Lists, Taxonomies, Lattices, Thesauri and Ontologies." Knowl. Org. 41 **3**.

Mike Conway, A. K., Fariba Fana, William Scuba, Melissa Castine, Danielle Mowery, Wendy Chapman and Simon Jupp (2016). "Developing a web-based SKOS editor." Journal of Biomedical Semantics: 9.

Open, O. (2017-2024). "Introduction to STIX." from https://oasis-open.github.io/cti-documentation/stix/intro.

Open, O. (2017-2024). "Introduction to TAXII." from https://oasis-open.github.io/cti-documentation/taxii/intro.

Sergio Caltagirone, A. P. a. C. B. The Diamond Model of Intrusion Analysis.

Stillions, R. (2014). "The DML model." from https://ryanstillions.blogspot.com/.

W3C (1994-2012). "Introduction to SKOS." from https://www.w3.org/2004/02/skos/intro.

W3C (2012). "OWL 2 Web Ontology Language Document Overview (Second Edition)." from https://www.w3.org/TR/owl2-overview/.