Ontology for Cybersecurity Governance of ICT Systems

Ontology for Cybersecurity Governance of ICT Systems

Fabio De Rosa[1,†], Nicolò Maunero[1,2,*,†], Luca Nicoletti[3,†], Paolo Prinetto[1,2,4,†] and Martina Trussoni[1,†]

[1]*Cybersecurity National Laboratory, Consorzio Interuniversitario Nazionale per l'Informatica, 25 Via Ariosto, Roma, 00185, Italy*

[2]*Politecnico di Torino, 24 Corso Duca Degli Abruzzi, Torino, 10129,Italy*

[3]*Agenzia per la Cybersicurezza Nazionale, 15 Via S. Susanna, 00187, Roma, Italy*

[4]*IMT Scuola Alti Studi Lucca, 19 Piazza S. Francesco, Lucca, 55100, Italy*

Abstract

Considering the continuous growth in the complexity of both information systems and security information, it becomes more and more necessary to provide solutions that facilitate the user in the management and use of these large and complex knowledge-bases. In the last years we have seen the birth of more and more examples that propose ontologies, semantically rich descriptions of entities and relations for the management of security information. The aim of this work is to provide an ontology that (i) supports a formal description of an ICT system, (ii) relates it to its potential vulnerabilities, possible attack vectors, and available mitigations, (iii) allows inferring a tight relationship between IT/OT assets and their vulnerabilities. Given the description of the ICT system, the ontology is automatically populated with security information items obtained by querying external knowledge bases (e.g., CWE, CVE, MITRE ATT&CK) and then providing the user with the necessary information to support operations such as Vulnerability Assessment and Penetration Testing and countermeasure planning.

Keywords

Knowledge-base, Cybersecurity, Ontology, Governance, Vulnerability

1. Introduction

Recent years have seen a continuous increase in cyber attacks, accentuated even more by the COVID-19 pandemic and the associated remote working[1]. Targets of attacks are the most disparate, from the single individual to large companies and public organizations, contributing to an annual cost, in terms of damage, of several billion (i.e., Wannacry alone resulted in costing companies more than $4 billion[2]). Therefore, it is becoming of crucial importance to put in place adequate defences to tackle an ever-evolving world.

Given the steady increase in cybercrime, governments in various countries have been prioritizing and strengthening investment plans to improve the security posture of the country's

ITASEC'22: Italian Conference on Cybersecurity, June 20–23, 2022, Rome, Italy

*Corresponding author.

†These authors contributed equally.

fabio.derosa@consorzio-cini.it (F. D. Rosa); nicolo.maunero@polito.it (N. Maunero); l.nicoletti@acn.gov.it (L. Nicoletti); paolo.prinetto@polito.it (P. Prinetto); martina.trussoni@consorzio-cini.it (M. Trussoni)

infrastructures, with particular emphasis on critical infrastructures. Notable examples are the 2017 executive order of the USA[3] and the European Union's NIS Directive[4], released in 2016 and its update (namely NIS 2) currently under review.

The need to guarantee predetermined levels of security and the constant growth of systems and digital infrastructures complexity makes it necessary, hence, to adopt technological solutions to support the management and governance of this information; security teams need to manage and correlate security data (i.e., vulnerability) and the infrastructure under analysis composition to identify vulnerable points and plan countermeasures.

In the last decade, ontologies have taken hold as means for the representation and semantically rich description, in terms of *entities - relations*, of complex knowledge-bases, especially, in the context of cybersecurity[5]. The use of an ontology allows a better categorization and, consequently, reasoning on the possessed data, as well as to represent and consider also the relations, explicit or implicit, between them[6]; the use of available reasoners[7] allows the identification of dependencies and non-explicit links between data in the knowledge-base, identifiable only after the population of the same.

The present paper presents a tool, based on the use of an ontology, for: (i) the identification of vulnerabilities in a system, (ii) the description of possible attack vectors for their exploitation, and (iii) the presentation of possible available mitigations.

To populate the ontology, security information is gathered by interacting with external knowledge-bases, such as CVE[1], NVD[2] and MITRE ATT&CK[3]. Once the ontology model is complete it is possible to reason over data, manually or automatically, to infer complex information about the infrastructure security; possible thanks to the tight relation between assets and their security information represented in the ontology.

The remainder of this paper is structured as follows. Section 2 provides an overview of the state of the art and related works, as well as information on the starting point of this work. Section 3 presents this work contribution, detailing the ontology and the solution developed. Section 4 depicts some use cases, while section 5 draws some conclusions and presents possible future works.

2. Background

The term *Ontology* has become commonly used in the field of computer science and engineering when talking about knowledge representation. An ontology is a formal description of a set of concepts belonging to the same domain. These concepts are clustered into classes and, for each class, the hierarchical relations linking it to the others (superclass - subclass) are established. The features and attributes of the different classes are called properties, the objects of the class are called individuals or instances and for each class the range of values that its instances can take is defined[8]. In this way, a knowledge-base of the domain of interest is created.

[1] https://cve.mitre.org
[2] https://nvd.nist.gov
[3] https://attack.mitre.org

2.1. ICT Ontology

With the Decree Law of 18 May 2018, n. 65, published on the Gazzetta Ufficiale n. 132 of 9 June 2018, Italy implemented the NIS Directive to define the measures necessary to achieve a high level of security of networks and information systems. The establishment of the Italian *Perimetro di Sicurezza Nazionale Cibernetica* (PSNC) takes place within the framework of the NIS Directive. The *PSNC* was established under Article 1, comma 1, of DPCM No. 105 of 21 September 2019, converted with amendments by Law No. 133 of 18 November 2019 (in the *Gazzetta Ufficiale* No. 272 of 20/11/2019) to ensure a high level of security of the networks, information systems, and IT services of public administrations, public and private entities, and operators having an office in the national territory, on which the exercise of essential State functions depends.

All of these entities, according to the Decree, are required to prepare and update, at least once a year, a list of the networks, information systems, and IT services for which they are responsible, including their architecture and components. They must, then, identify the ICT assets necessary to perform the essential function or service, in order to assess the impact of an incident on the ICT asset, in terms of its operability and of the compromise of data availability, integrity, or confidentiality (CIA triad) and assess dependencies with other networks, information systems, IT services or physical infrastructures of other entities. Finally, entities must identify the ICT assets that, in the event of an incident, would cause total disruption of the essential function or service.

In order to manage ICT asset information, the *Agenzia per la Cybersicurezza Nazionale* (ACN)[4] developed an Ontology, in the following referred to as `ICT Ontology`. It follows the guidelines of the DPCM and it allows compliance with the law by describing in a structured manner all the relevant components of the `Essential Function` and their relationships. In particular, it describe the architecture of the infrastructure and the relationships with other entities and external services.

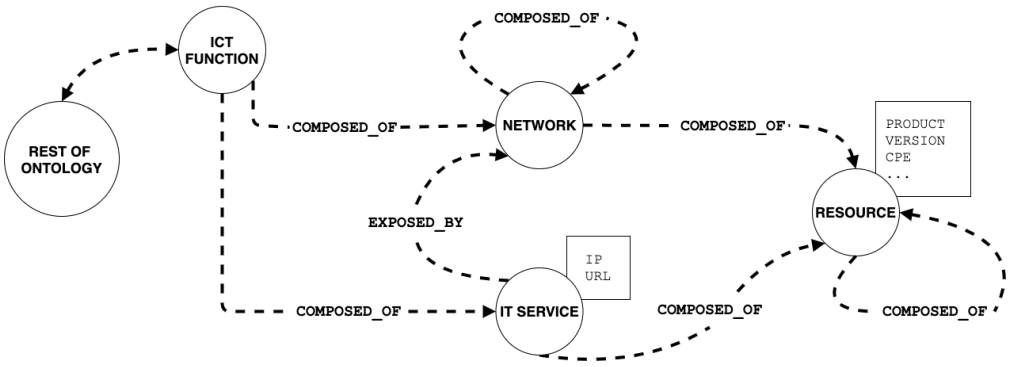

Figure 1: Partial Representation of the ICT Ontology.

Figure 1 partially depicts the structure of the ontology, highlighting the most important entities and relations:

[4] https://www.acn.gov.it

- `ICT Function`: identifies the infrastructure supporting the delivery of the essential function to be represented;
- `Network`: represents a network. Allows for the representation of the infrastructure internal and external connections;
- `IT Service`: represents a service that the essential function provides or a service provided by external entities on which the essential function relies;
- `Resource`: represents the resources composing the infrastructure. The entity is characterized by several properties allowing for the description of software and hardware resources. The picture shows some of them, including; (i) the product name, (ii) the software, or, more in general, the product version, (iii) the Common Platform Enumeration (CPE), i.e., a standard naming scheme introduced by NIST[5] for IT system, software, and hardware products identification.

2.2. Related Work

2.2.1. Cybersecurity Ontologies

The Unified Cybersecurity Ontology (UCO) [9] is an extension of Intrusion Detection System (IDS) ontology[10]; its objective is to bring forth a common and standard structure to describe the cybersecurity domain. The main idea behind the project is to change the approach of the cybersecurity standards from a syntactic representation to a more semantic one. A large number of existing standards and ontologies have been studied and reviewed and the most common ones have been selected to be integrated with UCO. In particular, UCO is intended to be the semantic version of *STIX*[11] integrating references to available external standards, i.e., CVE, CWE[6], CAPEC[7] and many others.

UCO is at the moment the most comprehensive and exhaustive ontology for cybersecurity related information and it has been mapped to all the most common publicly available ontologies, but for the work presented in this paper one fundamental aspect is missing: the description of the infrastructure. The focus of UCO is to give an overview of all general concepts in cybersecurity, including possible attacks, attack patterns, means and consequences, but only very few classes are dedicated to the description of the infrastructure.

Another notable work proposing a cybersecurity ontology is the Internet Of Things Security Ontology (IoTSec)[12]. The goal of the authors is to provide a means to represent and analyse information security information in the IoT field.

IoTSec introduces the concepts of `Asset` and `SecurityMechanism` that were not present in UCO and that help to outline an overview of an infrastructure. The project aimed at ensuring that companies in the Internet of Things field use their devices in the most secure possible way and at helping them to identify vulnerabilities and criticalities. Being IoT oriented, many subclasses of `Asset` are very specific, but the underlying idea of being able to describe the composition of the system in detail goes in the direction of the work presented in Section 2.1. The negative aspect of IoTSec is that the knowledge of the classes `Vulnerability` and

[5] https://nvd.nist.gov/products/cpe
[6] https://cwe.mitre.org/
[7] https://capec.mitre.org/

`Threat` is static: it is not designed to interact and comply with external sources and must be managed and maintained directly when implementing the ontology.

2.2.2. Security Assessment Ontologies

Considering previous works proposing the study, development, and use of ontologies for the management of security information of a system while leveraging on the knowledge-base for assessing the security and/or level of risk of a given infrastructure or system, the work of Rosa et al. [13] provides a good overview of major solutions available in the literature. More recent examples include, instead, the work of Venkata et al.[14] which proposes a framework for the security assessment of CPSs (Cyber Physical Systems). The proposed framework allows, through the use of tools developed by the authors, to identify system vulnerabilities and possible countermeasures. Security information and system data are loaded into the ontology designed to allow the reasoning about the impact that a vulnerability may have on the represented scenario. The proposed countermeasures are very simple and generic, i.e., patching the system, and are taken from a set defined by the authors to support their solution. Aouad et al. propose in [15] an ontology to support the developed risk assessment methodology for a computer system. The ontology in this case is used to organize the information necessary to carry out the operations of cyber risk assessment and tries to describe the relationships between the system, a threat, and the defensive measures currently in use.

3. Contribution

This section presents the work done. The objective is to provide a tool to support security operations that allows the analysis and management of related information:

- infrastructure composition in terms of assets, networks, functionality, and dependencies with external entities;
- information on system vulnerabilities;
- information on attacks and mitigation.

All this information items are organized in a semantically rich knowledge-base, built with the support of an ontology. The ontology is composed of three main parts, linked together by the relative relationships, which will be presented in more detail in the following sections:

- **ICT Ontology**: allows the description of the reference infrastructure;
- **Vulnerability Ontology**: contains and organizes data on the vulnerability of the infrastructure. It is populated thanks to the interaction with external databases such as CVE, NVD, and CWE;
- **Attack Ontology**: contains and organizes data on possible attacks, how a vulnerability can be exploited, and possible mitigations. Populated using information coming from the CWE and MITRE ATT&CK databases[16].

The ontology has been described using the OWL 2 language and resorting to Protégé, a tool developed by Stanford University[8].

[8] https://protege.stanford.edu

3.1. Improved ICT Ontology

The ontology composition, and the main rationale behind it, has been already presented in Section 2, but for this work, the available ontology has been slightly modified adding some additional entities and relations as well as reorganizing the structure of some entities to better represent the interaction with the rest of the ontology.

The first modification introduced some new classes and a novel hierarchical organization between some of the existing ones. In particular, some new concepts have been introduced, including:

- `Asset`: it is a general concept that includes any information system, device, or data that must be protected;
- `SecurityProperty`: it contains a set of individuals representing the main security properties that an asset may require, namely `AccessControl`, `Accountability`, `Anonimity`, `Authentication`, `Authorization`, `Availability`, `Confidentiality`, `Integrity`, and `NonRepudiation`.
- `SecurityMechanism`: it is a general class that is modelled to contain all the possible mechanisms put in place to protect assets.

The `Asset` class is related to the `SecurityMechanism` class through the object property `hasSecurityMechanism`. The `SecurityMechanism` class introduces some security mechanisms that are important when assessing the security of an infrastructure. All the new information are split into the following sub-classes:

- `CryptographicConcept`: it introduces in the ontology three key concepts of cryptography that are `DigitalSignature`, `HashFunction` and `KeyManagement`.
- `EncryptionAlgorithm`: it specifies the algorithm used when encryption is performed.
- `NetworkManagementSecurityMechanism`: it allows to represent the security mechanisms dedicated to networks. Its main sub-classes are `IntrusionPreventionSystem`, `IntrusionDetectionSystem`, `Proxy`, `ReverseProxy`, and `ServerSecurityMechanism`.
- `SecurityPropertyMethod`: it allows to represent security properties not described by other classes. Its main subclasses are `AccessControlMethod`, `AuthenticationMethod` and `IntegrityMethod`.
- `Protocol`: it specifies the protocol, either secure or not, adopted.

3.2. Vulnerability Ontology

As seen in Chapter 2, UCO and IoTSec use two different approaches for vulnerability representation. The goal of this work is to provide a trade-off between the two, to allow a complete and easily integrated solution.

The idea is to add to the `ICT Ontology` the concept of vulnerability that the various assets in the system may present; the class `Vulnerability` is put in relation with the classes `Asset` and `SecurityMechanism`:

- `Asset hasVulnerability Vulnerability;`

- `Vulnerability isVulnerabilityOf Asset;`
- `SecurityMechanism mitigates Vulnerability;`
- `Vulnerability isMitigatedBy SecurityMechanism.`

The class `Vulnerability` internally is composed of several sub-classes to describe its characteristics and represent the link with the external vulnerability databases: this will allow later to populate the ontology resorting to direct queries to these external knowledge-bases. Modeling of the `Vulnerability` class follows the UCO approach[9]: a sub-class for each external source is defined hierarchically organized, in particular the `Vulnerability` class is modelled to accomodate the information available from CVE, CWE and NVD[17]. Both *CVE* and *CWE* are implemented as sub-classes of `Vulnerability`, in this way they inherit the existing relationships of the class `Vulnerability` with the other classes in the ontology.

The CVE class has the data property `CVE_ID` where the ID of the vulnerability can be stored as a string; the CWE has an equivalent data property called `CWE_ID`. Both the classes have the data property CVSS where the severity score of the vulnerability, if present, can be stored. In a vulnerability assessment operation perspective this can be greatly beneficial to rank vulnerability by their severity score and prioritize mitigation operation within the infrastructure. The new schema of the ontology, highlighting the major addition, is depicted in Figure 2.

As a result of these improvements, the ontology now includes dynamic security information. Vulnerabilities can be added manually or automatically by scanning assets for known vulnerabilities. The IDs of these vulnerabilities are then saved and all the necessary information to represent actual relationships between vulnerabilities and infrastructure assets is derived from external sources. Details on how carrying out this procedure will be provided in the sequel.

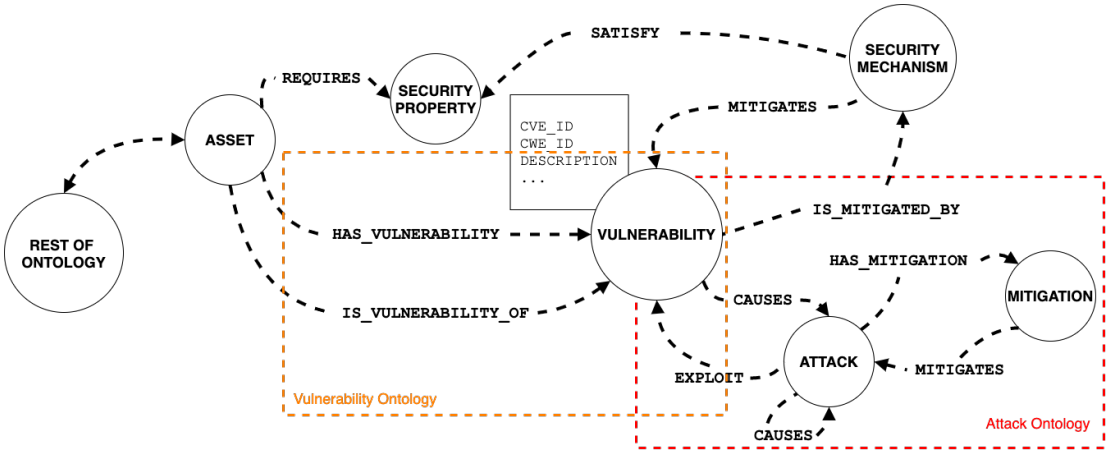

Figure 2: Defined Vulnerability and Attack Ontology.

3.3. Attack Ontology

Details and techniques used to perform penetration testing operations are out of the scope of this work, but we aim at providing, thanks to the ontology developed, a tool to support these type

of operations. Given a vulnerability of the system the tool can provide guidelines on how the vulnerability can be exploited by combining both technical information, such as those present in CWE in the form of code snippets, and cyber intelligence information describing more broadly how an attack can be carried out, the techniques used and so on, referring to the information provided by MITRE ATT&CK. In addition, the ontology also presents information on how a vulnerability can be mitigated, again leveraging primarily on the two resources indicated above.

To do this, the ontology `Attack` has been introduced and related to the other resources. It is linked just to the `Vulnerability` class through the following properties `Vulnerability causes Attack` and `Attack exploits Vulnerability`. Both these properties are linked also to the class itself, since an attack can leverage on another attack.

Moreover the `Mitigation` class is added, modelled to contain information about possible mitigation of the given vulnerability and attack. This class is put in relation with the `Vulnerability` class through the following properties: `Vulnerability has Mitigation` and `Mitigation mitigates Vulnerability`.

It is important to make a distinguo here: the classes `Mitigation` and `SecurityMechanism` seem similar, at least in relation to the `Vulnerability` class, but they are thought to accommodate and represent a different type of information:

- `Mitigation`: It is designed to be populated with information derived from vulnerabilities in the system. These represent potential methods to mitigate a given vulnerability, but which are not necessarily already implemented in the system.
- `SecurityMechanism`: It is designed to be populated when describing the infrastructure represented and contains information regarding the technologies adopted, at the time of compilation, in the system to secure it.

The development of the `Attack` and `Mitigation` classes follows an approach similar to the one used for the `Vulnerability` class, in fact, also these classes have been modeled starting from the information they must contain available in the external knowledge-bases.

Starting from the study of MITRE[18], the `Attack` ontology was modeled. In the work of MITRE, CVE entries are mapped to corresponding intelligence information contained in MITRE ATT&CK; the analysis of the impact on a system of each vulnerability is split into three steps: *exploitation technique*, *primary impact*, and *secondary impact*. Each of the steps refers to a particular ATT&CK technique, while the three steps represent the evolution of a possible exploitation of the vulnerability.

The `Attack` class is characterized by the following subclasses and relations:

- `TechniqueID`: represents the identifier of the corresponding technique in the MITRE ATT&CK database, internally the class also contains the reference to the sub techniques related to it;
- `TechniqueID has Technique`: represents how an adversary can achieve its goal;
- `Technique has sub-technique`: represents the relation with all the sub-technique it may have. Each sub-technique is characterized by its ID;
- `CWEID`: represents the identifier corresponding to the vulnerability in the CWE database;
- `CWEID has Example`: contains technical knowledge related to the CWEID entry. These contain pieces of code that can allow the identification and exploitation of the vulnerability.

The ontology includes also the class `Mitigation`, meant to be populated with the related information contained in MITRE ATT&CK and CWE. Therefore, it has been modeled accordingly:

- `TechniqueID`: represents the corresponding MITRE ATT&CK technique;
- `TechniqueID has PossibleMitigation`: describes possible mitigations for the particular technique;
- `CWEID`: represents the corresponding entry in the CWE database;
- `CWEID has PossibleMitigation`: describes possible mitigations for the particular CWE entry.

The new additions to the ontology are summarized in Figure 2.

3.4. Bundle Everything Together

Once the various pieces of the ontology have been completed and connected, all that remains is to fill the model with the necessary information.

Concerning the description of the infrastructure under analysis, this must be done manually to include the highest possible level of detail. On the other hand, information on vulnerabilities, attacks and countermeasures, are inserted in the ontology automatically thanks to available tools and ad hoc developed solutions.

For greater clarity, it is possible to distinguish two main phases that are carried out chronologically one after the other: first, the part of the ontology related to the system vulnerabilities is populated. The information entered within the `ICT Ontology` is used to query the available vulnerability databases and the collected information is entered into the `Vulnerability Ontology`. After this step, is then possible to query the CWE and MITRE ATT&CK knowledgebases to extract information regarding attacks and possible mitigation available, importing them within the `Attack Ontology`. The population process of the `Vulnerability Ontology` can be summarized in the following steps:

- If the CPE value of a product is available, then resorting to NVD can identify known vulnerabilities and extract the corresponding `CVEID`, `CWEID` and, if available, `CVSS` scores.
- If the value of `CPE` is not available then the CVE database can be queried directly using the product/vendor name and its version as the search key. In this case, the more details are available on the product, the more the search can be targeted and less wide-ranging. Once the entries of interest have been identified, the corresponding `CVEID` can be extracted and the NVD database can be queried to extract `CWEID` and `CVSS` score, if present.

Querying and interacting with the CVE database can be made more efficient by using the cve-search[9] tool, an open source project that consists of a local database that stores periodically synchronized information from CVE and a set of APIs to query the same. This allows faster queries and limits sending of sensitive information over the Internet. The interesting aspect is that the results can be collected in the MongoDB[10] format and through the use of another tool,

[9] https://www.cve-search.org/about/
[10] https://www.mongodb.com

M2Onto[19], it is possible to translate the information contained in a MongoDB directly into an ontology, after providing the tool with the ontological model to be filled.

The population process, on the other hand, of the `Attack Ontology` can be summarized in the following steps:

- Once the CVEIDs of all identified vulnerabilities are collected, resorting to the open source tool attack_to_cve[18] it is possible to extract the possible attacks related to the specific vulnerability. From here you can then extract the `TechniqueID` related to the attacks.
- Through the `CWEID` it is possible to query the corresponding database to extract the information necessary to populate the ontology, namely the classes `PossibleMitigation` and `Example` related to the corresponding `CWEID`.
- Through the `TechniqueID` identified above, it is possible to query the MITRE ATT&CK knowledge-base to extract the information needed to populate the ontology.

Once this process is completed, a knowledge-base of security related to the reference infrastructure is available to the user that can be used for security operations such as the identification of vulnerabilities present, the operations that can be done to exploit these vulnerabilities and related possible mitigations. In this particular case, the Protégé tool provides a convenient interface to query the ontology, but an automatic process has also been developed to extract the information collected and organize them in a report. Figure 3 outlines the overall scheme of the proposed solution.

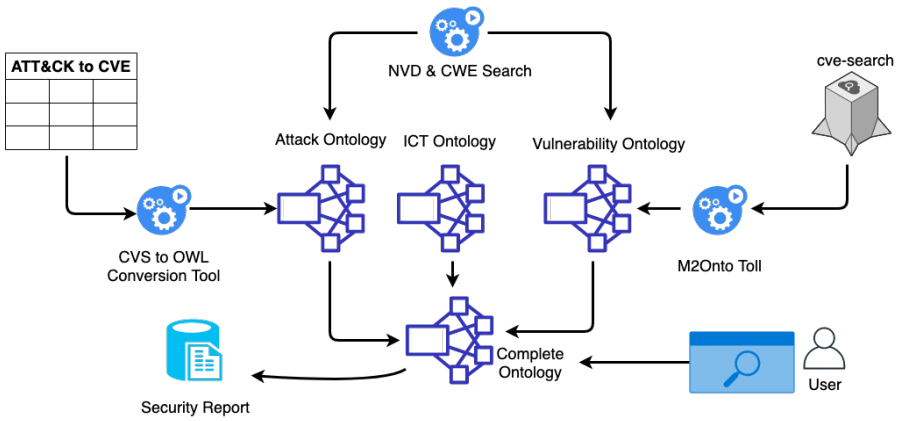

Figure 3: Proposed Solution

4. Solution Validation

The proposed solution, for its validation, has been used in different application contexts, for public and private operators identified as falling within the *Perimetro Nazionale di Sicurezza Cibernetica* and not. For secrecy and confidentiality reasons, the names and results obtained from the use of the system cannot be reported here.

5. Conclusion and Future Works

The paper presents the development of an ontology for the governance of data related to the security of an IT infrastructure, which allows to relate information about assets with vulnerabilities, attack vectors, and possible mitigations. Moreover, proprietary and non-proprietary tools for the automatic population of the ontology have been presented. The result is a system that allows the user to easily find and organize the information needed to plan operations such as VAPT and mitigation implementations to the identified vulnerabilities. Possible future developments, to improve the proposed solution, include:

- The use of tools to automate, at least partially, the population of the ontology related to the ICT system. These tools could include, among the other, asset management and discovery, and network scan tools.
- The integration into the ontology of the DFD (Data Flow Diagram) representation[20]. This addition will allow, leveraging on the ontology, to perform system threats modeling[21]. It will then be possible to use the ontology to support all the steps of Risk Assessment operations, from identification of threat to vulnerability assesment and penetration testing.

References

[1] Fortune, There's a huge surge in hackers holding data for ransom, and experts want everyone to take these steps, Available at https://fortune.com/2022/02/17/ransomware-attacks-surge-2021-report/, 2021. Accessed 20 April 2022.

[2] Kaspersky, What is WannaCry ransomware?, Available at https://www.kaspersky.com/resource-center/threats/ransomware-wannacry, ???? Accessed 20 April 2022.

[3] C. . I. S. Agency, Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, Available at https://www.cisa.gov/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure, 2017. Accessed 20 April 2022.

[4] Directive (eu) 2016/1148 of the european parliament and of the council of 6 july 2016 concerning measures for a high common level of security of network and information systems across the union, Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148, 2016.

[5] R. Aranovich, M. Wu, D. Yu, K. Katsy, B. Ahmadnia, M. Bishop, V. Filkov, K. Sagae, Beyond nvd: Cybersecurity meets the semantic web., in: New Security Paradigms Workshop, 2021, pp. 59–69.

[6] R. J. DeStefano, L. Tao, K. Gai, Improving data governance in large organizations through ontology and linked data, in: 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), 2016, pp. 279–284. doi:10.1109/CSCloud.2016.47.

[7] S. Abburu, A survey on ontology reasoners and comparison, International Journal of Computer Applications 57 (2012).

[8] N. F. Noy, D. L. McGuinness, et al., Ontology development 101: A guide to creating your first ontology, 2001.

[9] Z. Syed, A. Padia, T. Finin, L. Mathews, A. Joshi, Uco: A unified cybersecurity ontology, in: Workshops at the thirtieth AAAI conference on artificial intelligence, 2016.
[10] J. Undercofer, A. Joshi, T. Finin, J. Pinkston, et al., A target-centric ontology for intrusion detection, in: Workshop on Ontologies in Distributed Systems, held at The 18th International Joint Conference on Artificial Intelligence, 2003.
[11] S. Barnum, Standardizing cyber threat intelligence information with the structured threat information expression (stix), Mitre Corporation 11 (2012) 1–22.
[12] B. A. Mozzaquatro, C. Agostinho, D. Goncalves, J. Martins, R. Jardim-Goncalves, An ontology-based cybersecurity framework for the internet of things, Sensors 18 (2018) 3053.
[13] F. d. Franco Rosa, M. Jino, A survey of security assessment ontologies, in: World Conference on Information Systems and Technologies, Springer, 2017, pp. 166–173.
[14] R. Y. Venkata, P. Kamongi, K. Kavi, An ontology-driven framework for security and resiliency in cyber physical systems, ICSEA 2018 (2018) 23.
[15] L. Aouad, M. R. Asghar, Defender-centric conceptual cyber exposure ontology for adaptive cyber risk assessment., in: ICETE (2), 2020, pp. 580–586.
[16] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, C. B. Thomas, Mitre att&ck: Design and philosophy, Technical report (2018).
[17] R. Ushakov, E. Doynikova, E. Novikova, I. Kotenko, Cpe and cve based technique for software security risk assessment, in: 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), volume 1, IEEE, 2021, pp. 353–356.
[18] MITRE, Mapping mitre att&ck® to cves for impact, https://github.com/center-for-threat-informed-defense/attack_to_cve, 2022.
[19] H. Abbes, F. Gargouri, M2onto: an approach and a tool to learn owl ontology from mongodb database, in: International Conference on Intelligent Systems Design and Applications, Springer, 2016, pp. 612–621.
[20] Q. Li, Y.-L. Chen, Data flow diagram, in: Modeling and Analysis of Enterprise and Information Systems, Springer, 2009, pp. 85–97.
[21] OWASP, Owasp ontology-driven threat modelling (odtm) framework, https://github.com/OWASP/OdTM, 2022.