STIX-based theoretical framework for prioritizing relevant CTI Information

Victor Nazianzeno–Le Jamtel

Internship Report

Peter Hagstrom
Thesis Supervisor

RHEA SYSTEM B.V
JONCKERWEG 18
2201 DZ NOORDWIJK
The Netherlands

September 13, 2023

Glossary

asset Something of value for a company, including a software, hardware, program, database, critical information or research sample. While supporting assets are IT-specific infrastructures or software, primary assets are sensitive information and data. . 6, 15

CPE Common Platform Enumeration (CPE) is a structured naming scheme for information technology systems, software, and packages. . 15, 16, 23

CVE The Common Vulnerabilities and Exposures (CVE) system provides a reference method for publicly known information-security vulnerabilities and exposures.. 16

Target of Evaluation In accordance with Common Criteria, an information system, part of a system or product, and all associated documentation, that is the subject of a security evaluation. [7] . 15

threat Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability. [8] . 15

Abstract

The ever-evolving landscape of security threats requires a proactive approach to security management. This paper delves into the critical role of risk assessment in prioritizing threats within operational contexts. This study examines how the output of a threat risk assessment software can be leveraged to prioritize new threats and rank their relevancy in operational settings. The design, development and analysis of this framework is based on the RHEA-led SSE4Space software. SSE4Space is based on a Secure System Engineering framework and manages the risk assessment, development, maintenance and retirement of a mission's information system. In particular, the risk assessment step determines the security and business objectives, and defines threat scenarios that can be assessed in the context of the mission. The risk assessment framework provides security controls, threat models, scenarios and actors as well their link to the system's asset. The framework presented in this report makes use of this information from the risk assessment of SSE4Space in order to evaluate the relevancy of external, STIX-formatted cyber-threat intelligence in the context of a specific mission and system. In order to demonstrate the feasibility of the theoretical framework, a proof-of-concept (PoC) is provided, making use of a probabilistic Factor Analysis of Information Risk (FAIR) model in order to map both SSE4Space and the CTI's metrics into a single relevancy score. The output of the framework is evaluated qualitatively in order to demonstrate the meaning of the relevancy scoring, as well as the uses of this framework in an operational context.

Contents

Chapter 1

Introduction

Cyber risk assessment is a crucial step in understanding the impact of certain threats on an organization primary and supporting assets, on individuals and on operations. It assess the level of controls in a system, and how they affect the measured risk in order to obtain an acceptable level at the end of the cycle.

However, despite its significance, cyber risk assessment is often underutilized in operational contexts, such as in Security Operations Center (SOC) teams. While frameworks like SSE4Space are providing a continuous support to a mission's information system, there is a missed opportunity to integrate it into an operational context and provide many benefits, such as relevancy scoring of external threats, or de-noising indicators of compromise in cyber threats feeds. This missed opportunity can be attributed to the sparsity of research studies on the topic. A few articles [13] provide a high-level discussion on the strategic benefits of using a risk-based approach for prioritizing threats, however they remain abstract and don't provide a technical discussion on the topic.

Not using risk assessment to its full potential can lead to missed opportunities to prioritizing emerging threats and vulnerabilities. The manual assessment and prioritization of external Cyber Threat Intelligence might leave out important indicators of compromise, while incorporating noise into the Intrusion Detection Systems. Understanding the assets of a system through its vulnerabilities and its place in a threat model could lead to a more relevant assessment of external CTI beyond simply scoring threats on their severity. As a result, there is a clear rationale for integrating cyber risk assessment as a foundational aspect of continuous security operations.

This report is built upon the RHEA-led SSE4Space software, which supports the development, maintenance and retirement of the information system of spatial missions. In particular , it involves a risk assessment step for assessing risks in spatial missions using Secure System Engineering. This step establishes the security and business objectives of a mission, while also defining the potential threat scenarios that require evaluation. We further extend our investigation to leverage the data

generated from the risk assessment of SSE4Space, using it as a basis to evaluate the relevancy of external cyber-threat intelligence in a mission-specific and system-centered context. Since SSE4Space makes use of different catalogues, it provides an opportunity to score the relevancy of external threats on different levels (vulnerabilities, weaknesses, attack patterns) and map them to the threat modeling defined in the risk assessment step of SSE4Space.

In order to create a relevancy score that takes into account both the severity of the external threat, and the different metrics from the Risk Assessment Software, we will build a scoring model based on the Factor Analysis of Information Risk (FAIR) model. While this model is mainly use for risk analysis, we used custom metrics that can be mapped from the Risk Assessment software and the external threat. The use this model is enhanced by incorporating a Bayesian Network in order to be able to provide fuzzy metrics to the model. More precisely, a metric will not have a discrete state, but rather a probabilistic vector in order to fine-tune the scoring and take into account the uncertainty of certain metrics.

To demonstrate the practicality and efficiency of our theoretical framework, we present a proof-of-concept (PoC). This PoC employs a probabilistic Factor Analysis of Information Risk (FAIR) model, which facilitates the amalgamation of metrics from both SSE4Space and the Cyber Threat Intelligence (CTI) into a unified relevancy score. Subsequently, we assess the output of this framework through qualitative analysis, shedding light on the significance of the relevancy scoring and its potential applications within operational environments.

In a first chapter, we will discuss the background needed to be familiar with the notions discussed in this paper. In a second chapter, the design of the framework will be described, alongside its control flow and the meaning of each metric of the framework. To demonstrate the practicality and efficacy of our theoretical framework, we present a proof-of-concept (PoC) implementing it. A threat model will be presented for the Risk Assessment, and a STIX-formatted Threat Intelligence bundle will be used as the external threat to be scored for relevancy. Finally, we will discuss qualitatively the use of the framework, its compatibility with OWASP and SSE4Space, as well as the relevancy of the metrics. We will also discuss improvements and future works that could lead to a development for practical use.

Chapter 2

Background

2.1 The STIX language

A definition of the STIX language can be found on their website:

Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence (CTI).

STIX is an open-source framework developed by the OASIS foundation [11] and provides a global and deterministic way of sharing Cyber Threat Intelligence. The language is based on JSON format and allows sharing CTI in a consistent and machine-readable format.

Another widely used standard for CTI sharing is Malware Information Sharing Platform & Threat Sharing (MISP). STIX has a few advantages over MISP, such as its granularity, as well as its interoperability due to its standardized format.

There are 18 [10] STIX Domain Objects, including Attack Pattern, Threat Actor, Vulnerability or Malware. A Cybersecurity analyst can then build a report using those objects as well as specific relationships representing edges between objects. It allows a Cybersecurity expert to analyse CTI by considering data as graphs, and using graph theory to cluster, rank and explore threats when they arrive in a bundle.

More precisely, companies can use STIX to receive or share threats and collect indicators of compromises, which are artifacts suggesting a breach in a system or network. Then can then update their threat landscape and better analyse and detect incoming threats. As STIX can also define threat actors or campaigns, it provides a way of keeping track of recent threat actor's activities and their

targets.

2.1.1 STIX and OpenCTI

OpenCTI [4] is an open-source platform designed for Cyber Threat Intelligence (CTI) management and collaboration. It provides a structured environment for collecting, organizing, and analyzing threat intelligence data, enabling organizations to better understand and respond to cyber threats. OpenCTI facilitates collaboration among security teams, supports the integration of various data sources, and enhances the overall effectiveness of threat intelligence operations in the Cybersecurity landscape.

OpenCTI works with STIX-formatted data, and allows to treat them as graphs, enabling powerful data visualization. An example of such data can be seen in Figure 2.1

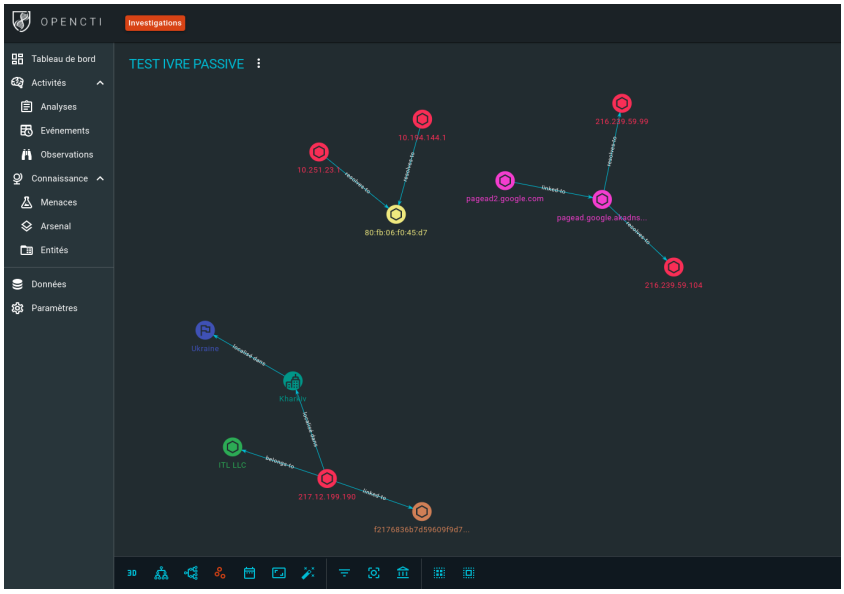


Figure 2.1: Example of an OpenCTI graph

OpenCTI is commonly used for threat hunting, as it easily integrates with TAXII feed [5] and is a great automation and visual tool for threat intelligence sharing. It also enables SOC to analyse malware, do reporting, and share IoCs from their local system or network.

2.2 Overview of SSE4Space

Secure Systems Engineering for Space (SSE4Space) is a framework for applying the security engineering process at a system level, during the whole life-cycle of a mission. SSE4Space uses the system's

context, as well as security and system objectives in order to perform threat modeling and assess the risk on different assets of the system. It is a continuous tool that provides risk assessment, and defines security controls and requirements in order to reduce the risk.

The framework is designed to integrate with the European Cooperation for Space Standardization (ECSS), a collaborative initiative aimed at developing and maintaining a set of standardized practices, guidelines, and requirements for space-related activities in Europe. These standards help ensure consistency, safety, and interoperability across European space missions and projects.

During the risk assessment phase of SSE4Space, threat scenarios involving different assets of the Mission are defined. For each scenario, a risk score will be computed using the OWASP [12] risk scoring metric. The process for which risk is evaluated is not detailed in this paper, as SSE4Space only serves as background information for the scope of the framework.

2.3 Risk-rating methods

Risk-rating models are quantitative frameworks used to evaluate and assign risk scores to various aspects of an organization's cybersecurity posture. These models analyze factors such as the organization's vulnerabilities, threat landscape, security controls, and potential impact of incidents. By assigning numerical or categorical risk ratings, they help organizations prioritize cybersecurity investments, make informed decisions, and allocate resources effectively to mitigate threats. The ratings provide a standardized way to communicate the level of risk to stakeholders and enable better risk management and decision-making in the context of cybersecurity.

The FAIR (Factor Analysis of Information Risk) model is a widely recognized and comprehensive risk assessment framework used to quantify and manage information security and cybersecurity risks. FAIR breaks down the risk assessment into essential components, including the identification of assets, threats, vulnerabilities, and potential impacts. It uses a quantitative approach to assign values to these components, enabling organizations to calculate and compare the financial impact of various risks.

In the FAIR model, risks are expressed in terms of probable frequency and magnitude of loss, resulting in precise understanding of potential exposures. This approach helps organizations prioritize security measures and allocate resources effectively by focusing on the most significant and impactful risks. FAIR's structured and quantitative methodology makes it a valuable tool for risk managers, allowing them to make informed decisions regarding cybersecurity investments and risk mitigation strategies. It enhances an organization's ability to assess and manage cybersecurity risks in a way that aligns with broader business objectives.

Both the FAIR (Factor Analysis of Information Risk) model and OWASP risk scoring model serve

as valuable tools in the field of cybersecurity, but they have distinct focuses and methodologies.

The OWASP risk scoring model primarily targets web application security and vulnerability assessment, providing a numerical ranking for vulnerabilities based on severity. It's particularly useful for developers and security professionals dealing with web application security.

On the other hand, the FAIR model offers a broader and more quantitative approach to risk assessment, encompassing information security risks across an entire organization. It evaluates risks in terms of financial impact and likelihood, making it highly suitable for risk managers and executives in decision-making roles. While OWASP specializes in web application security, FAIR provides a more comprehensive framework for assessing and managing information security risks throughout an organization.

The Loss Event Frequency (LEF) in the FAIR model quantifies how often a specific type of security incident or loss event is expected to occur within a given timeframe. It provides a numerical estimate of the likelihood of such events, helping organizations assess the frequency with which they may experience cybersecurity breaches or data breaches.

There are a few reasons to use the FAIR model, in particular the LEF, as a base for the Proof Of Concept of the framework described in this report:

- Risk-based threat prioritization is a new field in Cybersecurity, and research studies are sparse. Some valuable work has been done however on developing evidence-based threat prioritization [3] extending the FAIR model for this purpose.
- While OWASP mainly focuses on web application vulnerabilities, the FAIR model can be applied to any threat, and allows for a more modular use.
- FAIR's modularity also extends to its metrics. While FAIR defines some high-level metrics such as the LEF to describe likelihood, it is possible to extend the model by providing lower-level, more technical and concrete metrics. Such metrics are used in the framework describe in this report.

Chapter 3

Design

3.1 Focus on the likelihood

In the FAIR model, likelihood and Loss Event Frequency (LEF) are closely linked. Likelihood measures how likely a threat event is to happen, and LEF quantifies how often that event is expected to occur within a certain timeframe. The notion of timeframe refers to the fact that the different metrics are evaluated for a specific duration. For example, when evaluating a specific threat, it is possible to compute the Contact Frequency over a month, i.e. how many time a threat actor might interact with the target over a month. The timeframe is something qualitative that is decided before the FAIR analysis.

To conclude, likelihood forms the basis for calculating LEF in assessing cybersecurity risks, while LEF is an enriched way of considering likelihood by adding a temporal dimension.

When considering the relevance of a threat, the likelihood of it happening can often carry greater significance than its individual impact. This perspective arises from the recognition that even if a threat has a relatively low impact each time it occurs, if it happens frequently, it can accumulate into a substantial risk that poses significant harm to an organization. Therefore, evaluating the likelihood of a threat becomes essential in prioritizing it, ensuring that organizations address not only high-impact but also frequently occurring threats. In doing so, organizations can effectively manage risks that, over time, can have a considerable adverse impact on their operations and security.

To that extent, this framework will score and rank external threats based on their likelihood of happening based on the organization's profile.

3.2 Framework overview

A diagram representing the framework logic flow is shown on figure 3.1. The framework developed in this paper prioritizes threats on their likelihood only, as described in the previous section. The relationship between the framework scoring and the likelihood from OWASP will be detailed in the next section of the design chapter.

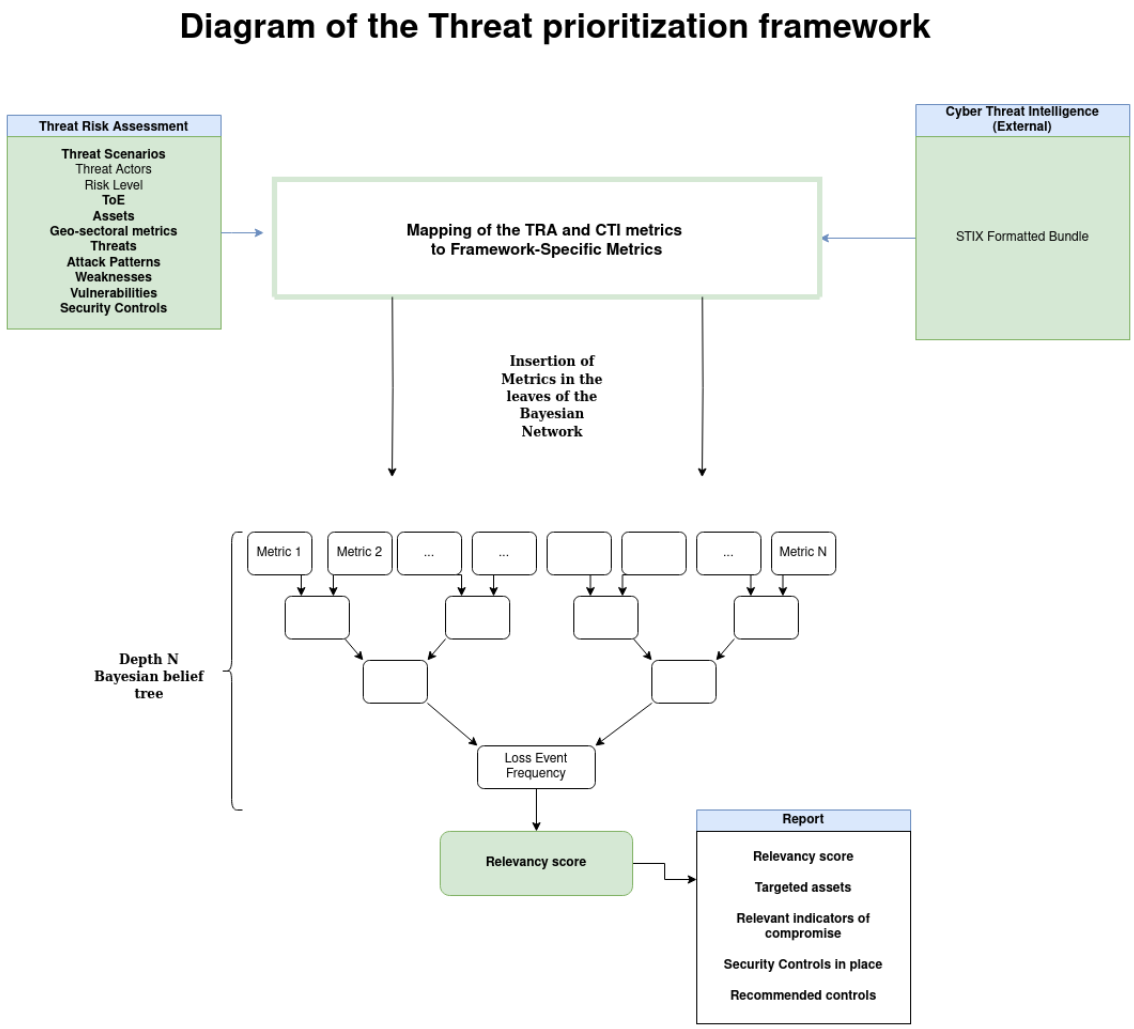


Figure 3.1: High-level diagram of the framework flow

We can describe the logic flow in the following steps:

- The external STIX-formatted threat bundle is divided into multiple clusters in order to identify

different threat actors, malware and campaigns.

- The framework iterates over the clusters and the risk assessment's data and extract the necessary information to instantiate each of the framework's metric.
- Once all of the metrics in the framework are mapped, they are inserted in the Bayesian network's leaves.
- The Bayesian Network then computes the root LEF score by performing Bayesian inference.
- The LEF vector is then converted to the relevancy score.
- Finally, the output contains the relevancy score, the identified IoCs for each cluster, the recommended controls and the controls in place as well as the targeted assets per cluster.

This enumeration gives a high-level view of the framework's flow. We will now describe each step more in details.

- The external CTI arrives as a STIX-formatted bundle. A community detection algorithm, namely the Louvain method, is applied on the bundle in order to cluster the STIX bundle around threat actors. This allows to separate different threat actors contained in a single bundle, and score them individually. The Louvain method is explained in details in the PoC chapter.
- For each cluster, an automatised mapping is made from it and the TRA to a list of set metrics. This list will be described in details later. While some metrics only relate to the TRA data, some of them are purely exclusive to the CTI, and a few are taking into account both of them, in order to evaluate matches on different levels. Each metric possesses 5 levels of severity, and quantitative thresholds are used for each in order to map the threat and the risk assessment data to the 5 levels scale.
- Once the metrics of the framework have been set, they are inserted into the leaves of a Belief Bayesian Network, on which we can perform probabilistic inference to compute the root of the tree, which in this case will be the relevancy score.
- Finally, alongside the relevancy score, a list of targeted assets, relevant Indicators of Compromise, security controls in place, and recommended controls are all added into a report which effectively prioritizes the threat by giving it a unique rank for the given mission.

3.3 Risk Assessment Metrics

The goal of the framework is to make use of the output of one **SSE4Space** Risk Assessment cycle in an operational context. More precisely, the framework aims at mapping an external threat alongside

the Threat and Risk Assessment (TRA) output to a unique relevancy scoring in order to prioritize the threat according to our mission and company data and metrics.

To that extent, an important step of designing the framework consists of mapping the output of an **SSE4Space**'s Assessment to the input of our framework, in a clean, concise and practical format. This mapping is not a transformation, but rather a reformatting, as we still use all the metrics from SSE4Space's risk assessment process. As risk assessment step was not designed to export data for such a specific use, it was necessary to refactor it and create a new data format and enriching it through the addition of a few attributes described in the following subsection.

3.3.1 Refactoring of SSE4Space's output

The following metrics from the Risk Assessment software were used in the new data format:

- **Threat Scenarios** are part of the threat modeling procedure in Risk Assessment. They consist of attack steps taken by a threat actor target a specific asset. It is important to include those scenarios in order to later map external threats to those, and assess their relevancy against our system. A Threat Scenario consists of a unique identifier, a textual description, as well as likelihood, impact and risk metrics. Moreover, threat scenarios include a threat actor, which is defined by its type, sophistication level, motivation and capabilities.
- **Target of Evaluation**: they consists of a system, or sub-system which can be targeted by an adversary. A ToE defines relationships between assets, as well as security objectives to guarantee confidentiality, availability and integrity to the included assets.
- **Assets** are crucial elements of the Risk Assessment data. We can distinguish supporting and primary assets. Supporting assets can be software, hardware, or a database that contains, manages or handles sensitive data or information for the company, called primary assets. Assets are referring to a list of ToEs as well as a list of Threat Scenarios to which they belong to. Assets have been enriched with additional attributes, as described in the next subsection.
- **Threats** are the core components of the threat scenarios. They are defined through techniques originating from catalogues , such as ATT&CK or SPACESHIELD.

3.3.2 Enrichment of SSE4Space

During the research step, a few attributes related to the risk assessment data were added.

- **CPE mapping**: One of the core aspect of the enrichment of the TRA is the addition of product enumerations linked to each asset. The CPE provides a list of software versions that can be

bilaterally linked with CVEs, i.e. known vulnerabilities. This allows to refer to an asset through its software version, as well as to link it to a known vulnerability and therefore evaluate its risk. CPE mapping can also come to be very useful for SSE4Space itself, as it would bind the assets to vulnerabilities through the CPE dictionary.

- **Geo-sectoral metrics**: In order to enrich the organization's profile, geographical and sectoral metrics were added on multiple levels of the risk assessment process. First, we added the organization's geographical profile containing the regions in which the mission take place, as well as the languages. Then, the organization's sectors were included as a list, containing sectoral keywords describing the scope of the organization (e.g. space engineering, spatial, aerospace, research and development). Finally, for each asset, geographical metrics are indicating its location, with different levels of granularity. For example, a web server can be located in Spain, while a database can be located in Köln, Germany. The addition of geo-sectoral metrics is relevant as it can match a threat actor's usual targets' profile. For example, if a threat actor is targeting spatial infrastructure in its campaigns, it will have increased relevance in regards of RHEA.

- **Enriched catalogue**: Having CPE-linked assets, it was then possible to enriched the risk assessment data by mapping each product version to a list of vulnerabilities. Those vulnerabilities were then mapped to known weaknesses (CWEs), providing a higher-level of abstraction as they don't relate to a specific software, but rather a faulty practice or a category of vulnerabilities. In a third entry, we added attack patterns (CAPEC), which are patterns used by malicious actors to exploit a set of weaknesses. Having a catalogue enrichment automatically inferred from the CPE entry allows to easily link an external threat to an asset, as long as this threat contains any kind of vulnerability, weakness or attack pattern. Therefore, we can link an asset to different levels of threats, not only vulnerabilities.

- **Security controls**: While security controls related to a scenario were already present in the original risk assessment data, some attributes were added in order to enrich the mapping with the external threats. More precisely, each identified threat / technique is assigned one or more security controls that mitigates it, with a *control strength* metric defining how efficient the control performs against this threat. The notion of control strength can refer as the efficiency of a control towards a specific threat. It can be assessed by an expert and would provide an indicative feedback on how the control managed to reduce the risk to an acceptable residual level.

  On another hand, SSE4Space's controls already include a boolean which determines whether a control has been already implemented in the system to mitigate a risk, or if it is still in progress. Our framework takes advantage of that boolean, either to tell the operational team that a control is already in place for the identified threat, or to give them a course of action in the mean of non-implemented controls.

3.4 Community detection

Louvain method is a community detection algorithm for extracting non-overlapping clusters from a graph [18]. While the mathematical details of the method won't be discussed here, it is important to note that Louvain method relies on the notion of modularity, which expresses the strength of division of a graph. More precisely, if a graph expresses high modularity, it means that there are highly connected nodes in each module, and every modules are sparsely interconnected.

Another key aspect is the fact that modularity takes into account the weights of the edges, which allows to center communities around specific nodes.

In the case of our framework, we chose to center the clusters around threat actors, malware, and campaigns. To do so, we gave more weight to relationships between such nodes and other objects. A visual explanation of Louvain method is given in the Proof-Of-Concept chapter.

3.5 Framework Metrics

This section aims at providing a detailed description of each metric of the framework, and how they are mapped from the risk assessment and the external threat data.

3.5.1 Overview

Figure 3.2 gives an overview of the metrics tree used for computing the relevancy scoring.

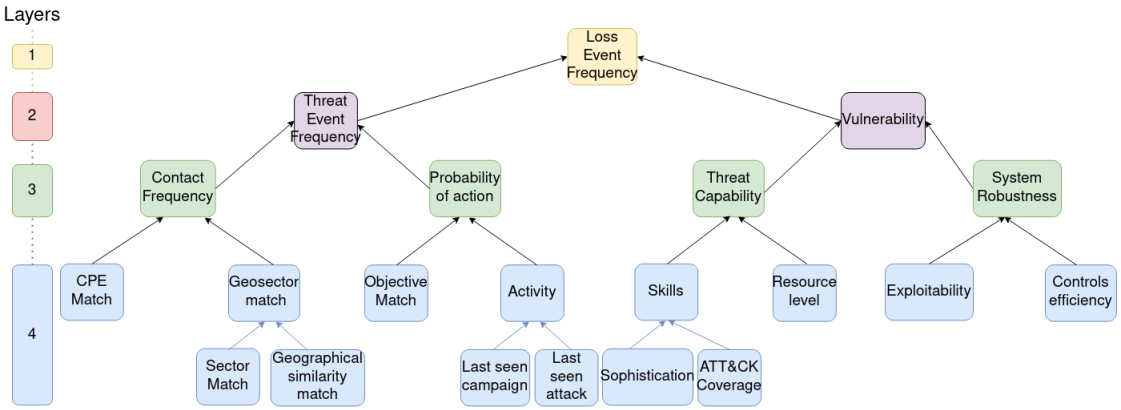


Figure 3.2: Overview of the metrics tree and their layers

We can distinguish metrics by their depth in the tree. The root on layer 1, namely the Loss Event Frequency, corresponds to the relevancy score for the likelihood. Layers 2 and 3 correspond to the

upper metrics, which are mapped from the FAIR model. Finally, the lower metrics in layer 4 are customized and mapped from the Threat risk assessment data and the external threat bundle.

3.5.2 Lower metrics

We can distinguish 14 lower metrics on the layer 4 of our framework.

- **CPE Match**: relates to whether the external CTI contains a threat targeting a software version present in the RA data. It contributes to the Contact Frequency Metric as a threat is more likely to interact with an organization if it is able to target its asset's software.
- **Geosector Match**: it is comprised of two submetrics, namely the sector match and the geographical match. The first one checks for sectoral keywords in the description of threat actors, campaigns or malware in the CTI, which the second one checks for linguistic or regional similarities between a threat's target and the RA data. A target with a matching geo-sectoral profile is more likely to be approached by a threat actor, which is why it contributes to the Contact Frequency.
- **Objective match**: this metric compares the goals of threat actors and campaigns in the external threat with the threat scenarios defined in the risk assessment software using string matching. If the goals of a threat actor is matching the description of an organization's system, it is more likely to take action against it, therefore it contributes to the Probability of Action.
- **Activity**: consisting of the last seen campaign and the last seen attack. This metrics extract timestamps and evaluate how recent the campaign, attack, or threat actor's activity is. The timestamps can be found in STIX-formatted data, especially in threat actors, campaigns, malware and intrusion sets. It contributes to the probability of action as a recent activity might indicate that the threat actor will attack in the near future.
- **Skill**: this metric describes the skill level of a threat actor. It looks at it sophistication level, as well as the ATT&CK Coverage. The latter corresponds to the number of techniques employed by a threat actor in term of the ATT&CK catalogues. It is an indicator of the capabilities of the malicious actor. Sophistication and ATT&CK coverage are complementary. The first one describes the level of skills an actor possesses, i.e. the complexity of the potential actions it could take, while the second metric evaluates the breadth of its skills, or the span of the techniques in possession of the actor, linked with the ATT&CK catalogue. The skill contributes to the threat capability, as it evaluates how effective an attack against a target can be.
- **Resource level**: the resource level determines the size of a threat actor, or its scales. It is often related to the identity which relates to the threat actor, ranging from an isolated individual to a nation-wide hacker team. It contributes to the Threat Capability metric as it evaluates the physical means of a threat actor, and is complementary with its skills.

- **Exploitability**: exploitability corresponds to a CVSS metric taken from CVEs. It indicates how realistic the exploitation of a certain vulnerability is. It inversely contributes to the System robustness, as a more exploitable system will lose in robustness.
- **Controls strength**: this metric takes into account the implemented security controls in the risk assessment software for the given threat model. It takes into account the controls applied to matching threats also found in the external CTI bundle. In other words, for a given threat, it will evaluate the controls matching this threat and average them into a single score. It contributes to the system robustness, as more controls help mitigate the risk of an asset being exploited successfully.

3.5.3 Upper metrics

Upper metrics have a much stronger semantic meaning. They are taken from the FAIR model, as well as a from a paper which implements evidence-based threat prioritization using FAIR [3]. We can use the definition given in this article as their meaning and usage in the framework are identical.

- **Contact frequency (layer 3)**: The probable frequency with which a threat actor will come into contact with an asset. It takes into account the CPE match and the Geosectoral match.
- **Probability of action (layer 3)**: The probability that a threat agent will act against an asset once contact has occurred. It includes the objective match and the activity metric.
- **Threat Event Frequency**: The probability that a threat actor will act against an asset. It is composed of the contact frequency and the probability of action.
- **Threat Capability (layer 3)**: The probable level of force a threat agent is capable of applying against an asset. It uses the skill and resource levels of threat actors identified in the bundle.
- **System Robustness (layer 3)**: this metric has been customized in order to accommodate the mapping from both the risk assessment and the external threat. It corresponds to the strength of the system in term of its exploitability and the implemented controls.
- **Vulnerability**: The probability that the threat actor's actions will be successful. It depends on the threat actor's capabilities, as well as how robust the system is.

3.5.4 Loss Event Frequency

The relevancy score corresponds to the root of the tree. The metric in place is called the *Loss Event Frequency*, which is defined in [3] as:

the probable frequency within a given time frame with which a threat agent will inflict harm on an asset.

It is important to note the probabilistic dimension here, which refers to likelihood. This is the subject of the next section.

3.6 Scoring

3.6.1 Relevancy score and likelihood

Limitations on likelihood

As stated at the beginning of this chapter, the development of the relevancy score in this framework is based on a notion of likelihood only. A first reason is that the work done in the evidence-based prioritization article [3] is also centered around the notion of *Loss Event Frequency*, which determines the probability of an asset being successfully targeted in a given time frame. Another reason was due to temporal constraints, as the development of the framework as well as the proof of concept took place during 7 weeks.

Impact, on the other side, could be linked to the severity of a threat. The final relevancy score, if taking into account both the likelihood and the impact, could be the product of these 2 metrics, similarly to computing risk. In that case, the likelihood would designate the relevance of a threat in regards to the organization's profile, while the impact would evaluate its severity. The likelihood would then then prioritize threats in a first step, and the impact could add another layer of prioritization by ranking relevant threats among themselves.

Relevancy defined with likelihood

Relevance, in the context of an cyber threat intelligence, refers to how pertinent a specific threat is to the system in question, taking into account the system's unique characteristics, assets, and vulnerabilities and the threat scenarios defined preemptively. A relevant threat is one that poses a direct and significant risk to the system's integrity, confidentiality, or availability. It is also one that is tied to the organization through the motivation of the threat actor, its targeted sector, or its geographical characteristics. On the other hand, likelihood assesses the probability of the threat materializing, considering various factors such as historical data, threat actors' capabilities, and the robustness of the system. There is a clear intersection between relevance and likelihood, even though it might not form an exhaustive relevancy assessment.

3.6.2 Bayesian Belief Networks

Using a probabilistic structure like Bayesian networks for prioritizing threats offers several advantages. Firstly, it allows for a more nuanced and flexible assessment of risks by incorporating probabilistic metrics, enabling organizations to account for uncertainties in their threat assessments. Secondly, Bayesian networks can model complex dependencies between various threat factors, providing a more realistic representation of how multiple threats can interact and compound each other's impact. Lastly, this approach enables continuous monitoring and adaptation as new data becomes available, allowing organizations to dynamically adjust their threat prioritization strategies in response to evolving threat landscapes.

Mathematically, a Bayesian network as a probabilistic graphical model defining variables that are related by conditional dependencies (conditional probability table). In the case of this framework, we apply the idea of a Bayesian Network to the FAIR model by having a directed binary tree topology, starting from the leaves to the root (see figure 3.2).

There are two advantages to using Bayesian networks in this context.

- Given a subset of variables having a state, we can infer the other variable's states probabilistically. In the context of this paper, it means that starting from the leaves, we can probabilistically infer the value of the relevancy score.
- Each variable / metric has a state. We consider 5 states, namely (very) low, medium and (very) high. Using a bayesian network, it is possible to enhance this discrete characterization by using multiple state for a single metric. For example, a metric can now be 60% low, and 40% very low. This fine tuning can increase the accuracy of the final score as this allows to refine the mapping from the risk assessment metrics as much as we want with respect to this 5-states scale.

The use of the FAIR model is not necessarily essential to the development of the framework. Indeed, FAIR is simply an ordering of metrics which allow risk to be analysis with respect to an asset. However, if FAIR was chosen, it is because some research has been done in threat prioritization using FAIR by incorporating Bayesian networks in the procedure.

3.6.3 Probability table

In order for the Bayesian network to be functional, it needs to rely on conditional probability tables. In the case of a binary-tree topology, conditional tables are defined for a variable and its two parents. For example, a table is defined for the activity, and its two parents, namely the last seen campaign and the last seen attack.

The probability table is derived from the influence of each of the parent metric on its child metric. Modifying those influence tables results in a different scoring, as they are setting weights for computing the score itself. The conditional probability tables can be computed from the influence tables using the regression method described in this article [6].

Those tables are specific to a mission, and need to be set up by an security expert beforehand, in order to specify how influential each metric is in the tree. This is one of the only step of this framework which needs some expert interaction, as it doesn't rely on the risk assessment data, but rather exists as a complement of it to rank threats relevancy.

Once the conditional probability tables are set, the Bayesian Network can perform inference by applying Bayes formula [16] on each node and therefore probabilistically inferring the state of the root node, given the states of the lower metrics.

3.7 Output

The output of the framework consists of 4 elements, namely the relevancy score, the list of Indicators of Compromise, the targeted assets and the recommended and implemented mitigation controls. The main attribute is the relevancy score for each detected community in the STIX-bundle. The other attributes were deemed useful for an operational context. This is discussed in later chapters.

3.7.1 Relevancy score

After obtaining a probability vector from the Loss Event Frequency, we can perform a weighted sum [6] to obtain a unique score. The weights are used to normalize the results, but don't affect how threats are ordered. In other words, the LEF vector is already prioritizing threats by itself, however, we compute this sum in order to obtain a scalar score.

Formally, we have the probability vector $\mathbf{v} = [v_l, v_l, v_m, v_h, v_h]$ and the weight vector $\mathbf{w} = [1, 2, 4, 8, 16]$. The weighted sum is given by:

$$\sum_{i=1}^{5} v_i \cdot w_i = v_l \cdot 1 + v_l \cdot 2 + v_m \cdot 4 + v_h \cdot 8 + v_h \cdot 16$$

This score is then normalized to a scale from 0 to 10, taking into account the distribution of the Bayesian network inference output. This is discussed in details in the Proof-Of-Concept chapter.

3.7.2 Indicators of Compromise

Each bundle consists of 0 or more indicators of compromises. They consists of hashes, ips, or URL that indicates a threat or malware present in the bundle. In STIX, they come with a pattern that can be used in an Intrusion Detection System in order to spot suspicious IP addresses, or files going through an organization network.

The IoCs of each cluster are added to the output alongside the relevancy score.

3.7.3 Products enumeration

As discussed earlier, CPEs are software versions linked to an asset in the risk assessment data. Therefore, if a product version was identified in the external threat, either through a vulnerability or an attack pattern, the corresponding asset will be included in the output. The report then includes the targeted assets alongside its CPE entries.

3.7.4 Mitigation controls

In the risk assessment output, there a controls listed for each threat. When finding a matching threat or technique in the external CTI, it is then possible consider which controls have been implemented to mitigate the threat, and which controls can be recommended in order to provide the operational engineer a course of action.

In order to match a control to a threat, it is possible to refer to the NIST 800-53 framework [2], which provides controls that can be mapped to the ATT&CK catalogue. While some controls might not be applicable to our systems, it still provides a course of action that will guide the operational team as it can link the mitigation to an asset.

Chapter 4

Proof-of-Concept

The Proof-Of-Concept (PoC) presented in this report is essentially an application of the framework with an example Risk Assessment JSON file and a example STIX-formatted CTI bundle. We will begin by presenting the scenario and the context of the PoC, before describing the threat scenarios and the threat modeling phase. We will then view the CTI bundle and observe how each metric is mapped, and how each cluster within the bundle is scored. We will briefly go through the output of the framework as well, and discuss the scoring distribution and how to normalize it.

4.1 Scenario

4.1.1 Description

AstraCorp is a R&D company dedicated to space engineering and space-compatible nano-components. It collaborates with public institutions on a research-level, as well as for database management. The company's goal is to perform research on different fields related to space engineering, as well as to store sensitive mission data for processing and testing. AstraCorp also works with private stakeholders investing money in Space R&D. AstraCorp possesses a Cybersecurity department, with a Risk Assessment as well as an Operational teams.

4.1.2 Context

Astracorp works with the public institution GovSpace for R&D purposes. The following primary and supporting assets are used in their collaboration:

Primary assets

- Sensitive data about mission samples
- Medical histories of astronauts

Supporting assets

- Webserver used for querying data in HTTP.
  - cpe:2.3:a:hypr:keycloak-authenticator:-:*:*:*:*:*:*:*
  - cpe:2.3:a:f5:nginx:1.1.1:*:*:*:*:*:*:*
- Web application made with node.js.
  - cpe:2.3:a:openjsf:express:4.3.1:*:*:*:*:node.js:*:*
  - cpe:2.3:a:nodejs:node.js:6.2.1:*:*:*:lts:*:*:*
- Database for AstraCorp sensitive data storage
  - cpe:2.3:a:oracle:mysql:8.0.18:*:*:*:*:*:*:*
- Cloud for Medical histories
  - cpe:2.3:a:microsoft:azure-open-management infrastructure:-:*:*:*:*:*:*:*

4.1.3 Threat Actors

Advanced

We define an advanced threat actor TA1-ADV whose goal is to access and leak sensitive data from GovSpace's cloud.

- adversaryType: spy
- sophistication: strategic
- opportunity: high
- motivation: critical
- capabilities: critical

We define an advanced threat actor TA2-ADV whose goal is to access and leak sensitive data from AstraCorp's database.

- adversaryType: crime-syndicate
- sophistication: expert
- opportunity: high
- motivation: critical
- capabilities: high

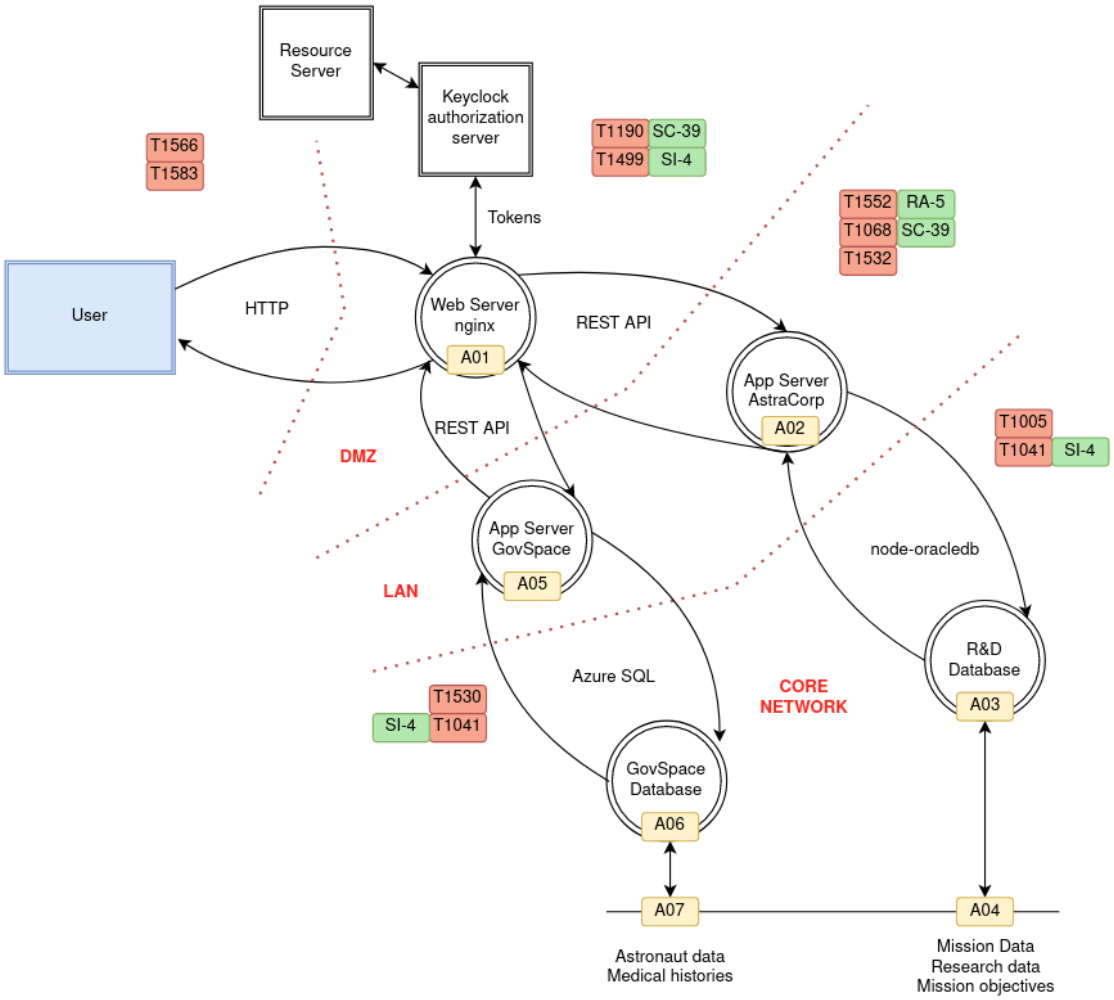
Intermediate

We define an intermediate threat actor TA3-IN whose goal is to prevent accessibility through denial of service of the nginx webserver.

- adversaryType: hacker
- sophistication: advanced
- opportunity: medium
- motivation: high
- capabilities: medium
- threatVectors: DENIAL-OF-SERVICE

4.2 Threat Model

The Threat Model can been seen in the following figure:



Label	Caption	Adversaries
T1566.002	Spearfishing links	TA1, TA2, TA3
T1552.001	Credentials in Files	TA1, TA2
T1068	Exploitation for Privilege Escalation	TA1, TA2
T1530	Data from Cloud Storage	TA1
T1005	Data from Local System	TA2
T1532	Archive collected data	TA1, TA2
T1041	Exfiltration Over C2 Channel	TA1, TA2
T1583.007	Acquire Serverless Infrastructure	TA3
T1190	Exploit Public-Facing Application	TA1, TA2, TA3
T1499.003	Application Exhaustion Flood	TA3

Table 4.1: Threat model captions

The red labels designate techniques from the ATT&CK catalogue, while the green labels are

controls from NIST 800 – 53. Finally, the yellow labels are assets. The name and description of each threat,control and asset can be found in the risk assessment JSON file on the github repository (see Appendix).

4.3 CTI Prioritization

4.3.1 STIX graph

Figure 4.1 shows the CTI bundle.

Figure 4.1: CTI graph for the Proof Of Concept

We can extract the following information from it.

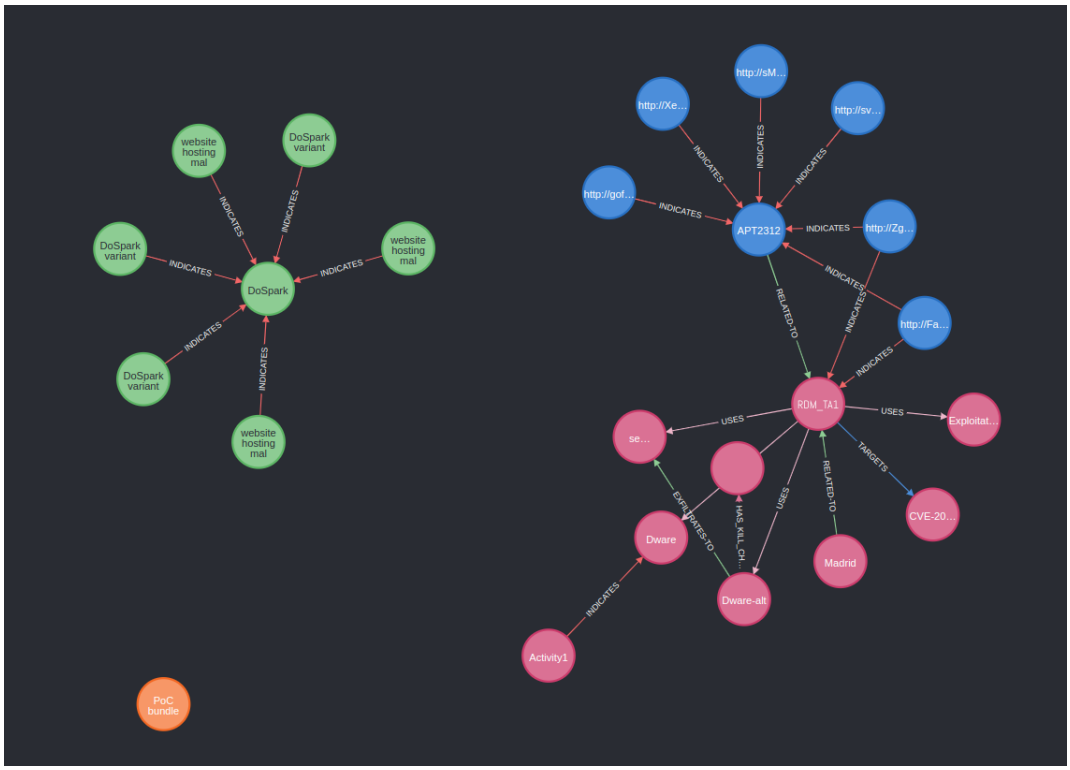
- The graph is partitioned.
- The first subgraph contains a malware and IoCs.
- The second graph is more complex, and contains a threat acotr (Artemis), an intrusion set (APT), a few malware linked to the threat actor, a vulnerability and attack pattern, an infrastructure hosting a malware, and many IoCs.

It would seem like the bundle could be separated into 3 communities based a first view of the components and their relationships, as the intrusion set and the threat actors seem to have an associative relationships, but not any kind of inheritance.

4.3.2 Clustering

In order to cluster the graph using Louvain method, we mapped the STIX bundle to a neo4j graph using a script. This script can also be found on the repository with a ".cypher" extension, and can be applied to any graph. Indicator relationships have lower weights than the rest, in order to center the clusters around threat actors and malware. In the PoC, the weights are set to 10 for the IoCs relationships, while the rest of the relationships weights are set to 50. This is a qualitative choice, resulting from manual testing on the efficiency of the clustering algorithm.

Having mapping the bundle to neo4j, we obtain the following clusters:



- The green cluster contains a Malware and IoCs. It is centered around the malware, since it is an isolated graph.
- The blue cluster centered around an imaginary APT adversary, namely **APT2312**. It also contains IoCs, and is related to a Threat Actor. This relationship is simply associative, in the sense that the APT and the Threat Actors are just "related to" each other.
- The pink cluster contains a Threat Actor, two malware, an infrastructure hosting a malware, an attack pattern as well as a vulnerability and a few indicators of compromise. It is a more exhaustive cluster, and is clearly centered around the threat actor since it possesses a relationship with all the objects within it.

Centering around threat actors is relevant for later scoring, since the threat actor is usually the most connected object in the graph. It can be correlated with how it relates to each type of object. For example, a malware is often used by a threat actor, while a vulnerability is often targeted by it. An IoC can indicate a malware used by the threat actor, which establishes an indirect composition relationship.

4.3.3 Scoring of each bundle

We will now look at how each metric from the framework is scored and how it extracts the data form the risk assessment file and the external CTI cluster. As a reminder, each metric can be a discrete scalar having 5 states, namely:

- Very Low: The metric shows very low relevance of the threat to the system
- Low: low relevance
- Medium: Significant relevance of the threat in regards of this specific metric
- High: Very significant relevance
- Very high: Critical relevance of the threat on that metric

While some metrics are scored using one such state (e.g. CPE match is High), some others can have fuzzy scoring, i.e. they can be represented as vectors that sum up to 1. An example could be that the sophistication level of a threat actor is $[0, 0, 33\%Medium, 0.67\%High, 0]$. It allows to account for a more precise mapping, as well as for uncertainties regarding some inputs.

- **CPE Match**: The framework extracts the vulnerabilities from the external threat, finds a catalogue entry and compares it to the risk assessment's vulnerabilities. If there is a match, it looks at which CPE entry it corresponds to, and then finds the CPE match. The CPE match is medium with one match, and increases state to High and Very High with aditional matches.
- **Sectoral Match**: The framework looks for the textual description of threat actors, identities, campaigns, and malware in the bundle. For each of them, it compares them with keywords that would indicate a sectoral match. Those keywords are defined in the framework, and depends on the mission's scope. The algorithm used for this is the Levenshtein heuristic [17] which compares strings character per character. Sectoral match is high after one keyword match, and very high after two.
- **Geographical Match**: The framework looks for linguistic or regional matches between threat actors, malware, identities, campaigns and the risk assessment's geographical metrics. Similarly to the sector, it will parse the description of those objects, as well as the location attributes

of identities and STIX Location objects in order to find a string match for a language or a region / city. The scoring is Medium after one keyword match, and increases one level per additional match.

- **Objective Match**: The framework compares the textual goals of threat actors and campaigns with the description of the threat scenarios in the risk assessment. The Levenshtein metric is computed between 0 and 1, and mapped to a 5-level scale into a vector in order to provide a fuzzy scoring to account for inaccuracies or false positives.
- **Campaign Activity**: The framework extract timestamps of threat actors, campaigns and intrusion sets. The scoring is given by the average of all the timestamps and the most recent one, and is mapped to a 5-level scale which is defined between a day and a year. This scale can be modified depending on the time frame chosen by the analyst. For example, an APT might be active less frequently but over a longer time frame, which would still be very relevant.
- **Attack Activity**: Similarly to the campaign activity, the framework looks for timestamp in infrastructure, malware and related IoCs. The scoring method is the same.
- **Sophistication**: The threat actors in STIX possesses a sophistication metric which refers to their skill level in term of hacking competences. This 7-level scale is then mapped to a 5-level scale in the framework
- **ATT&CK Coverage**: The framework parses techniques and attack patterns in the bundle. It scores this metric depending on the number of matching techniques and AP with the risk assessment data. The match is performed with catalogue entries (ATT&CK, but could extend to SPACESHIELD and SPARTA).
- **Resource Level**: The Resource level refers to the size of the threat. In STIX, it is represented by a textual attribute, from script kiddies to nation-scale adversary. It is a field in the Threat Actor object. This scale is then mapped to the 5-level scoring of the framework.
- **Exploitability**: The framework looks for matching vulnerabilities in the threat cluster, and average their exploitability metric, which is a mandatory field of the CVSS scoring for CVEs [1].
- **Controls strength**: The framework finds matching attack patterns and techniques in the bundle, and extract the control strengths attribute of the risk assessment data, and average them. Note that in that case, it also checks that the control strengths are belonging to implemented controls, using the **implemented** Boolean in the risk assessment security controls objects.

We can see on Figure 4.2 the scoring for the cluster containing the threat actor RDM-TA which specifically targets aerospace and governmental telecommunications infrastructures.

- Sectoral match is high due to the identified sectors in the threat actor's goals.

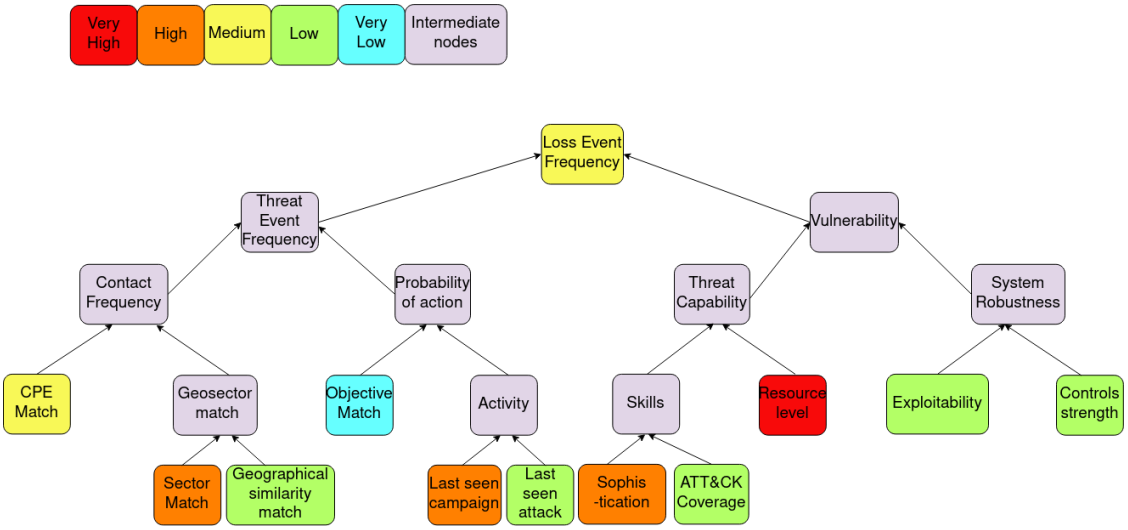


Figure 4.2: Scoring of the threat actor cluster from the PoC

- Resource level is high, as actor is identified to be part of a government team
- Objective match is very low, due to the lack of similarity with any of the threat scenarios in the risk assessment data.
- CPE match is medium, which means that a vulnerability has been identified in the threat, and it is targeting a specific asset's software version from our system.

4.4 Framework I/O

4.4.1 Command Line Interface

The framework is designed in Python and uses a command-line interface in order to score a bundle in two steps. The Proof-Of-Concept contains a *main.py* file which is the script launching the framework computations using two arguments.

- **python3 main.py cluster** will instantiate a Neo4j server with the given credentials present in the file. It will then parse the URL of the CTI bundle also given in the file and convert the bundle into a Neo4j format using a script. Once on Neo4j, the framework will launch a script to cluster the bundle using Louvain's method, as described above. Finally, python will parse the clustered graph and split the bundle into the different clusters.
- **python3 main.py score** will open the clusters file, and score each cluster according to the scoring system described above. It is required to be run after the first command in order to

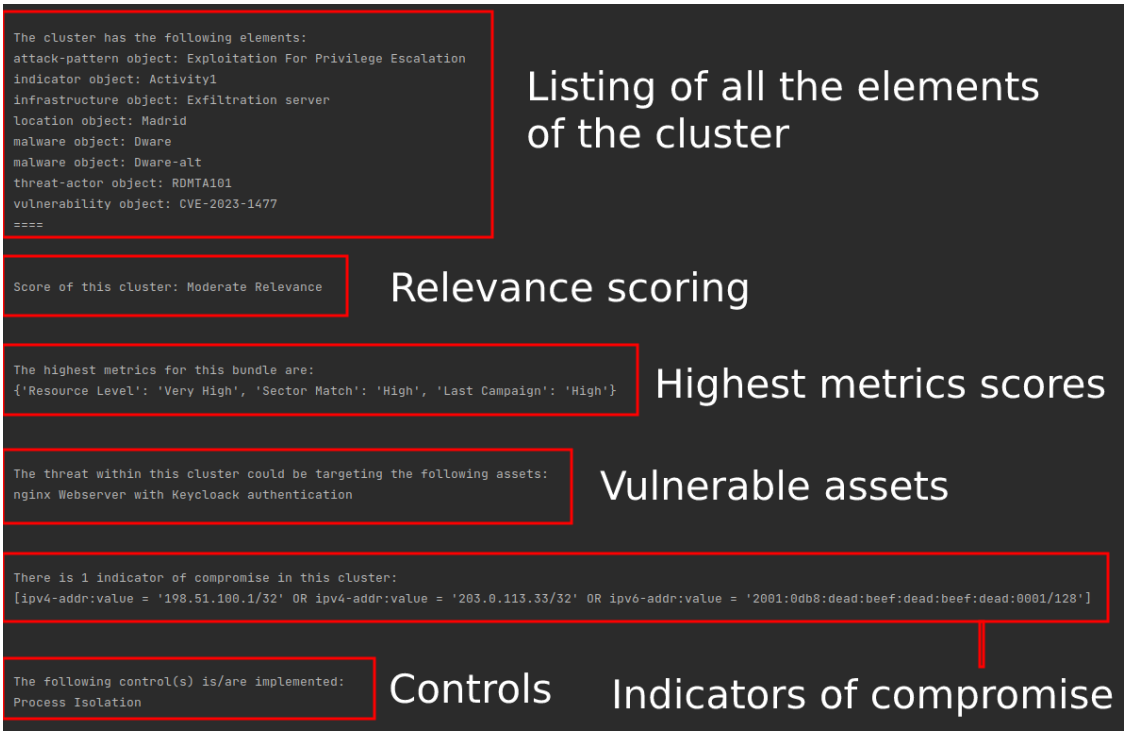


Figure 4.3: Example output of the framework

first cluster the bundle.

4.4.2 Format

Once the scoring is done, the framework outputs the different information described in the previous chapter. Figure 4.3 shows and explains the different parts of the output of the framework with one of the cluster in the Proof-Of-Concept.

4.4.3 Scoring distribution

In order to to map a score to a relevancy level, it is important to understand the distribution of the Bayesian Tree outputs, as it is unlikely they will follow a normal distribution. After obtaining the LEF, a post-processing step was made in order to normalize the output distribution. This is especially important as in future works, when considering the impact metric in the relevance scoring, it would be necessary to have a fixed bound for the likelihood and the impact in order to obtain an overall score that is also bounded for a given mission.

The Bayesian network inference was ran on 50,000 random samples to approximate the distri-

bution of values for the final LEF score. In other words, the base metrics received a random score between 0 and 4, and Bayesian Inference was performed to compute the *LEF* score based on those metrics. The resulting approximated distribution is shown on Figure 4.4

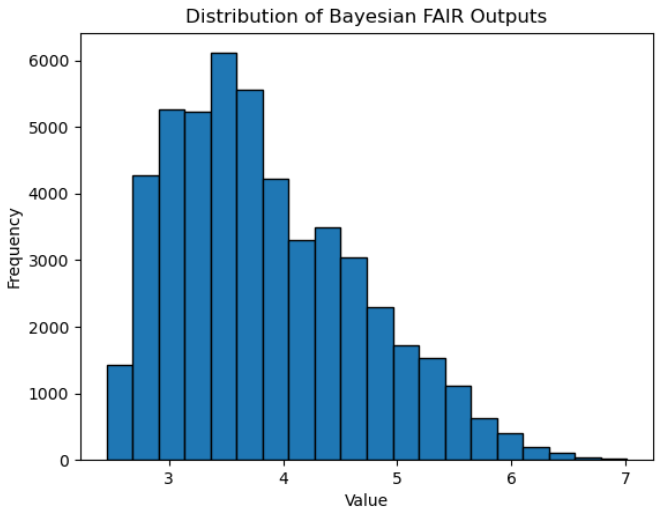


Figure 4.4: Distribution of values for the LEF score

It is clear that the distribution is centered around 3.5, and is not uniform, especially on higher values. The lower and upper bounds are respectively 2.5 and 7. In order to convey a meaningful mapping to relevancy, the scoring output was normalized before being assigned a relevancy label.

This can be approximately achieved using percentile ranking [19], which, for a given value in a distribution, calculates the percentage of scores that are less than that value. The percentile graph can be seen on Fig 4.5.

In order to convince ourselves that this technique does approximate to a uniform distribution, we can plot the percentiles in term of their frequency, shown on Fig 4.6

The normalized output of the Bayesian Tree then allows to define meaningful thresholds for relevancy. For simplicity, we defined 4 thresholds at $0.2, 0.4, 0.6$ and 0.8. They create 5 intervals mapped to relevancy labels, ranging from **Very Low Relevancy** to **Very High Relevancy**. For example, if a bundle is ranked at 0.53, it will receive the **Medium Relevancy** label.

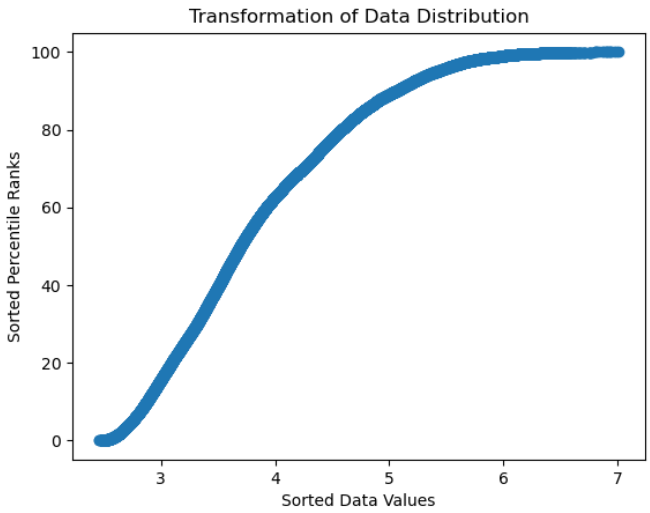


Figure 4.5: Percentile rank for LEF values

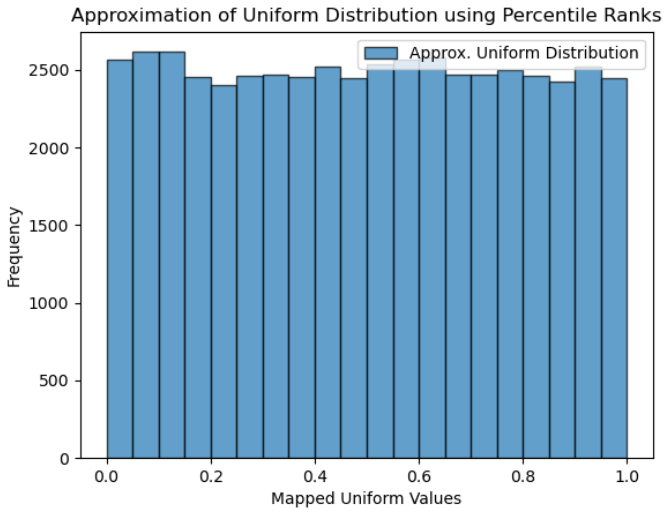


Figure 4.6: Percentile frequencies

Chapter 5

Discussions

5.1 Qualitative Assessment of the Proof Of Concept

There are a few reasons why a quantitative assessment of the PoC would bring much relevance to its evaluation.

- The scoring system relies on qualitative factors and primarily relies on refining the probability tables within the Bayesian network. The fine-tuning of the influence matrices of the Bayesian network is not a subject of evaluation for this report.
- As this theoretical framework is an innovation and is not supported by many research studies, it is difficult to perform a comparative study and therefore assess quantitatively the efficiency of the framework.
- Given that the PoC is an fictional example, it is more suitable to be evaluated through a qualitative analysis, using hypothesis on test-cases.

In order to analyse qualitatively the PoC, we will use the following test-case in order to understand whether the scoring is relevant given the metrics, the context of the external CTI and the data from SSE4Space.

5.1.1 Test-case: RDM-TA threat actor

We can focus on the third cluster from the PoC. It can be found in the Appendix B at the end of the report, in JSON STIX format. The different objects within the cluster are listed in Figure 5.1.

When focusing specifically on the threat actor, we can find the following attributes:

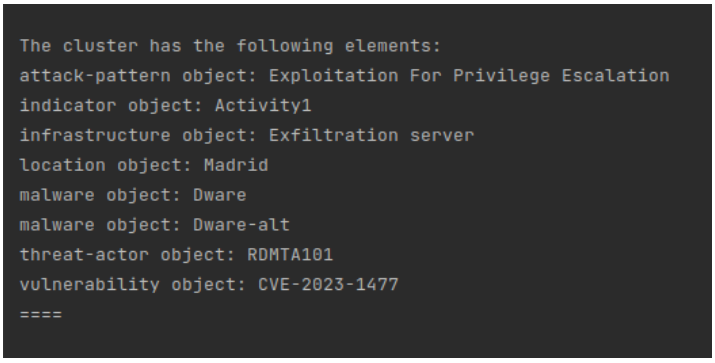


Figure 5.1: Objects contained in the cluster 3 from the PoC


```
"threat--3451f6c6-f512-5c53-956b-1c3cd5c7b06b": {
        "name": "RDMTA101",
        "threat_actor_types": [
            "spy"
        ],
        "last_seen": "2023-08-01T09:49:00.000Z",
        "roles": [
            "malware-author"
        ],
        "goals": [
            "RDMTA101 has been identified as a group of cyber- criminals tied with the
set. They are known for having authored several malware, in particular used for data exfil
        ],
        "sophistication": "expert",
        "resource_level": "government",
        "primary_motivation": "organizational-gain",
        "secondary_motivations": [
            "dominance"
        ],
        "personal_motivations": [
            "notoriety"
        ],
        "type": "threat-actor"
    }
```


We can make the following observations regarding how relevant this threat actor is, and more generally the whole cluster:

- The textual goals contain many keywords such as aerospace, government, telecommunica-

tions etc... They could indicate a high sectoral match.

- The threat actor's sophistication is very high, which would be mapped directly in the corresponding metric.
- the resource level is also high
- the threat actor's last activity is recent, and would indicate that it is still active.

On the output of the CTI, we observe the following highest scored metrics:

- Resource level: Very High. In STIX, a government-scale resource level is considered to be critical, or very high.
- Sophistication: High: the Expert level of sophistication in the 7-level STIX scale is mapped to high in our 5-level scale.
- Sector match: High: at least 3 keywords have been found in the threat actor goal's itself, indicating a high sectoral match.

It is important to understand that while in that case the threat actor contributes greatly to the cluster's score, in other instances, other objects, such as malware, campaigns or even infrastructures could have a higher influence, depending on their metric matches or their attributes. In the case of this cluster, the threat actor was very central to the cluster, and the other objects, such as malware, had a minor contribution to the overall scoring, notably with the timestamp extraction or the resource level.

5.2 Utility of the model for Operational Use

5.2.1 Recommended and Implemented mitigation

In an operational cybersecurity context, having lists that outline both the implemented controls associated with identified threats within each cluster and the recommended controls derived from the risk assessment serves several valuable purposes.

Firstly, the implemented mitigation list offer a clear and concise overview of the protective measures currently in place, facilitating quick and effective responses to potential threats. They serve as valuable reference points, aiding security teams in promptly assessing the impact of a threat, and realistically assessing its severity given the relevancy score.

Additionally, the inclusion of recommended controls, encompassing non-implemented measures identified during the risk assessment, could enhance the security strategy. By highlighting

areas where enhancements are needed, these recommendations enable the operational team to prioritize and strategize their security efforts effectively in regard of how relevant or severe the analysed threat is. Providing a course of action would give a starting point to evaluate the security controls strategy, and would work in complement of the business objectives in order to provide reasonable and adequate safeguards.

5.2.2 Vulnerable assets

In an operational context, having a list of potentially vulnerable assets per cluster generated by the framework offers several advantages. Firstly, it provides a targeted and prioritized focus on areas of heightened risk, enabling security teams to allocate their resources more efficiently and effectively. Since the operational team can prioritize the threats using the relevance score, it can then prioritize the assets to be protected instead of simply relying on vulnerabilities catalogue. Secondly, this list could help in the rapid identification and remediation of vulnerabilities, minimizing the attack surface to potential threats. Lastly, it facilitates ongoing monitoring and risk mitigation efforts, allowing organizations to adapt and evolve their security measures to address emerging cyber threats and changes in their operational landscape.

5.2.3 Indicators of Compromise

Prioritizing a threat effectively leads to the prioritization of its Indicators of Compromise (IoCs), which, in turn, helps in reducing noise in Intrusion Detection Systems (IDS) and other security mechanisms for several reasons. When a threat is given precedence, security teams can focus their monitoring and detection efforts on the specific IoCs associated with that threat, thus reducing the volume of alerts generated by unrelated or less critical events. This targeted approach streamlines the allocation of resources and allows for more efficient use of personnel and technology. Additionally, by concentrating on high-priority threats and their IoCs, security teams can respond more swiftly and decisively to potential incidents, enhancing overall threat detection and response capabilities while minimizing the false positives among the noise of lower-priority alerts.

Moreover, when combining the implemented controls with the IoCs, an operational team can also decide whether the IoCs would have any use, if they deem that the controls are sufficient and would mitigate the external threat.

5.3 Comparison with other Threat Prioritization Frameworks

The sparsity of research studies in risk-based threat prioritization reflects a gap in cybersecurity knowledge and practice. Despite the growing complexity of cyber threats, limited research has been

dedicated to developing comprehensive methodologies for effectively assessing and prioritizing these threats based on the risk assessment of an organization's system.

We can summarize the work of Ondra Rojčík on developing Priority Intelligence Requirements (PIRs) for an organization [14].

Priority Intelligence Requirements (PIRs) are directly linked to threat prioritization in cybersecurity, as they define the specific information needs that inform the ranking and focus of security efforts on the most critical threats.

In the theoretical framework developped in this article, a few points can be summarized:

- Threat prioritization, similarly to the framework presented in this report, results from the analysis of an external threat, and the risk assessment from the company.
- Contrary to our framework, many steps involve an expert judgment or approval. This is one of the main contrast, as our framework focuses mainly on automation, and on scoring threats arriving in streams, i.e. asynchronously. On the other hand, the RedHat framework is comprised of many synchronous steps, with expert approval and manual mappings, which makes the process less suitable in an operational context, but potentially much more accurate.
- The frameworks has a concentric consideration of assets. Valuable assets, mostly the primary ones, such as sensitive information, are considered crown jewels, and are at the heart of the security implementations. It can be argued that overprotecting the crown jewels might have a high financial impact in term of security measures, while the attack surface on assets such as web servers will be greater, as they might be under-protected due to their external concentric position. Therefore, the RedHat frameworks applies prioritization to assets on a first place, rather that on threats themselves.
- Geographical metrics can be irrelevant if the organization's profile is too diverse. The same can be said to sectoral metrics, and this actually represents one of the limitation of our Proof Of Concept.

Chapter 6

Future Work and Improvements

6.1 Suggestions for SSE4Space

The development of this framework also had the side-effect of finding possible relevant changes that could be applied to SSE4Space.

- **CPE mapping**: linking assets to vulnerability is current done manually in SSE4Space. For each asset, a set of vulnerabilities is taken from different catalogues, and are then used in the threat scenario to evaluate the impact of a threat on the asset, given its vulnerabilities. An idea that was developed in this framework was the addition of one or more CPE entries linked to each asset. For example, if a system is composed of a web server, it is possible to link it with a precise CPE entry describing the software version. This link allows to automatically map vulnerabilities to assets, as the CVE catalogue contains CPEs entries for each vulnerability [9]. This improvement could help analysts and security expert to find more relevant vulnerabilities when performing risk assessment, and end up with more concrete results as the vulnerabilities are linked to the exact software version that is used in the mission.
- **Geographical and sectoral metrics**: enriching the organization profile with geographical and sectoral data would allow a more specific and possible more accurate risk assessment step, and would be overall beneficial for supporting the mission's whole lifecycle. This data would allow organizations to understand region-specific cyber threats and industry-specific attack patterns, enabling the customization of security protocols accordingly. Furthermore, it supports proactive threat detection and response, strengthening overall cyber resilience and minimizing the risk of security breaches.

6.2 Fine-tuning of the Metrics

There are many improvements that can be done on the scoring algorithm of the framework, both on Bayesian tree metrics and the mapping performed beforehand.

- The FAIR model is not necessarily the best match with the current risk assessment method. Indeed, as SSE4Space currently uses OWASP-based risk scoring, it would be more meaningful to score the relevancy through the OWASP likelihood and impact metrics. The tree structure as well as the bayesian network model could still be used, as only the metrics would change.
- The current mapping from the risk assessment data and the external threat to the framework metrics can also be improved. For the moment, the framework uses thresholding to score a specific metric. For example, it considers that after a certain number of sectoral matches (i.e. the threat actor targets at least 2 matching sectors), the sector metric will be set to High. While this can be backup by qualitatively assessing how many sector matches can make the threat relevant for the mission, the scoring still needs to be more formalized in order to be integrated in a full software in the future.
- Several metrics are semantic-related, like the geographical, sector and objective matches. They rely strictly on string matching for the moment, and it allows the algorithm to find keywords that are almost or completely identical between the risk assessment data and the external threat geo-sectoral targets and goals. This matching could be improved by using Natural Language Processing [15], by performing semantic analysis on the description of malware, threat actors and campaigns in the STIX-formatted CTI.

6.3 Feedback loop

* reinforcement learning on the influence matrix *reinforcement learning on the cluster algorithm by checking previous bundles and creating connections to new ones to have more meaningful clusters at the end, therefore the relevancy is more accurate. * future work on NLP

also add: * future work on kill chain phase

Chapter 7

Conclusion

* bridges between risk assessment and CTI

Bibliography

[1] URL: https://nvd.nist.gov/vuln-metrics/cvss.

[2] *Complete 8500 Control List — stigviewer.com*. https://www.stigviewer.com/controls/800-53. [Accessed 07-09-2023].

[3] *Evidence-Based Prioritization of Cybersecurity Threats — isaca.org*. https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/evidence-based-prioritization-of-cybersecurity-threats. [Accessed 07-09-2023].

[4] *GitHub - OpenCTI-Platform/opencti: Open Cyber Threat Intelligence Platform — github.com*. https://github.com/OpenCTI-Platform/opencti. [Accessed 05-09-2023].

[5] *Introduction to TAXII — oasis-open.github.io*. https://oasis-open.github.io/cti-documentation/taxii/intro.html. [Accessed 11-09-2023].

[6] Anhtuan Le, Yue Chen, Kok Keong Chai, Alexandr Vasenev, and Lorena Montoya. "Incorporating FAIR into Bayesian Network for Numerical Assessment of Loss Event Frequencies of Smart Grid Cyber Threats". In: *Mobile Networks and Applications* 24.5 (Sept. 2018), pp. 1713–1721. DOI: 10.1007/s11036-018-1047-6. URL: https://doi.org/10.1007/s11036-018-1047-6.

[7] NIST. *target of evaluation (TOE) - Glossary | CSRC*. [Online; accessed 4-September-2023]. 2023. URL: https://csrc.nist.gov/glossary/term/target_of_evaluation.

[8] NIST. *threat - Glossary | CSRC*. [Online; accessed 1-September-2023]. 2023. URL: https://csrc.nist.gov/glossary/term/threat.

[9] *NVD - Full Listing — nvd.nist.gov*. https://nvd.nist.gov/vuln/full-listing. [Accessed 08-09-2023].

[10] OASIS Cyber Threat Intelligence (CTI) TC. *STIX™ Version 2.1*. [Online; accessed 2-September-2023]. 2019. URL: https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html.

[11] *OASIS Open Home - OASIS Open — oasis-open.org*. https://www.oasis-open.org/. [Accessed 10-09-2023].

[12] *OWASP Risk Rating Methodology | OWASP Foundation — owasp.org*. https://owasp.org/www-community/OWASP_Risk_Rating_Methodology. [Accessed 05-09-2023].

[13] *Prioritizing Vulnerabilities : A Risk Based Approach — threatintelligence.com.* https://www.threatintelligence.com/blog/vulnerability-prioritization. [Accessed 10-09-2023].

[14] Ondra Rojčík. URL: https://www.first.org/resources/papers/cti22-berlin/Ondra-Rojcik.pdf.

[15] *Semantic Features Analysis Definition, Examples, Applications — spiceworks.com.* https://www.spiceworks.com/tech/artificial-intelligence/articles/what-is-semantic-analysis/. [Accessed 08-09-2023].

[16] Wikipedia contributors. *Bayes' theorem — Wikipedia, The Free Encyclopedia.* [Online; accessed 11-September-2023]. 2023. URL: https://en.wikipedia.org/w/index.php?title=Bayes%27_theorem&oldid=1174313870.

[17] Wikipedia contributors. *Levenshtein distance — Wikipedia, The Free Encyclopedia.* [Online; accessed 12-September-2023]. 2023. URL: https://en.wikipedia.org/w/index.php?title=Levenshtein_distance&oldid=1169975534.

[18] Wikipedia contributors. *Louvain method — Wikipedia, The Free Encyclopedia.* [Online; accessed 7-September-2023]. 2023. URL: https://en.wikipedia.org/w/index.php?title=Louvain_method&oldid=1173553358.

[19] Wikipedia contributors. *Percentile rank — Wikipedia, The Free Encyclopedia.* [Online; accessed 31-August-2023]. 2023. URL: https://en.wikipedia.org/w/index.php?title=Percentile_rank&oldid=1158568027.

Appendix A

Project repository

The Proof-of-Concept is hosted in a private repository available here. In case you need access to the repository, you can contact the author at **v.nlejamtel@gmail.com**.

Appendix A

STIX-formatted CTI clusters


```
{
  "attack-pattern--5d2a0e29-a53f-5e67-b604-668b3e1daa7a": {
      "id": "attack-pattern--5d2a0e29-a53f-5e67-b604-668b3e1daa7a",
      "spec_version": "2.1",
      "revoked": false,
      "confidence": 75,
      "created": "2023-08-28T12:09:01.514Z",
      "modified": "2023-08-28T12:12:36.380Z",
      "name": "Exploitation For Privilege Escalation",
      "description": "The use of Dware also allows RDMTA101 to gain privilege within
      "x_mitre_platforms": [
          "linux",
          "windows"
      ],
      "x_mitre_id": "T1068",
      "x_opencti_id": "c68e19cf-78bd-45ad-9e14-268168e03660",
      "x_opencti_type": "Attack-Pattern",
      "type": "attack-pattern"
  },
  "indicator--f6d0c5d3-2b5d-5eb9-9cf9-63892891d74c": {
      "id": "indicator--f6d0c5d3-2b5d-5eb9-9cf9-63892891d74c",
      "spec_version": "2.1",
      "revoked": false,
      "confidence": 75,
      "created": "2023-08-28T12:23:00.570Z",
      "modified": "2023-08-28T12:23:00.570Z",
      "pattern_type": "stix",
```

```
        "pattern": "[ipv4-addr:value = '198.51.100.1/32' OR ipv4-addr:value = '203.0.1
        "name": "Activity1",
        "valid_from": "2023-08-28T12:23:00.564Z",
        "valid_until": "2023-10-27T12:23:00.564Z",
        "x_opencti_score": 50,
        "x_opencti_detection": false,
        "x_opencti_main_observable_type": "IPv4-Addr",
        "x_opencti_id": "11bd4484-1f44-41ec-b056-3b93519ca8bd",
        "x_opencti_type": "Indicator",
        "type": "indicator"
    },
    "infrastructure--509eb5e5-10b9-525c-8ba8-c342c51c4b45": {
        "id": "infrastructure--509eb5e5-10b9-525c-8ba8-c342c51c4b45",
        "spec_version": "2.1",
        "revoked": false,
        "confidence": 35,
        "created": "2023-08-30T07:23:57.409Z",
        "modified": "2023-08-30T07:24:25.254Z",
        "name": "Exfiltration server",
        "description": "External server used by RDMTA101 to exfiltrate data to. The li
        "infrastructure_types": [
            "exfiltration"
        ],
        "last_seen": "2023-02-15T23:00:00.000Z",
        "x_opencti_id": "976223d9-c738-4a91-bd17-14d8981bd67f",
        "x_opencti_type": "Infrastructure",
        "type": "infrastructure"
    },
    "location--69b20db1-498b-59d4-8b79-83eee0456cff": {
        "id": "location--69b20db1-498b-59d4-8b79-83eee0456cff",
        "spec_version": "2.1",
        "revoked": false,
        "confidence": 15,
        "created": "2023-08-28T12:18:33.527Z",
        "modified": "2023-08-28T12:19:47.511Z",
        "name": "Madrid",
        "description": "Capital of Spain. Investigations have shown with medium confid
        "latitude": 40,
        "longitude": -3,
        "x_opencti_location_type": "City",
```

```
        "city": "Madrid",
        "x_opencti_id": "d075e5d8-2dec-4c5e-aa8f-59849a739207",
        "x_opencti_type": "City",
        "type": "location"
    },
    "malware--a9ad4436-8488-5db7-82ac-28a818faf27b": {
        "id": "malware--a9ad4436-8488-5db7-82ac-28a818faf27b",
        "spec_version": "2.1",
        "revoked": false,
        "confidence": 75,
        "created": "2023-08-16T13:33:51.062Z",
        "modified": "2023-08-16T13:45:24.676Z",
        "name": "Dware",
        "description": "Dware (or D-ware) is a malware used by RDMTA101. It leverages
        "malware_types": [
            "backdoor"
        ],
        "is_family": false,
        "architecture_execution_envs": [
            "x86-64"
        ],
        "x_opencti_id": "9e74c89e-7787-49d5-a540-cae895bd3a85",
        "x_opencti_type": "Malware",
        "type": "malware"
    },
    "malware--b9ae3909-bea0-5146-8a0a-f7cf869026a7": {
        "id": "malware--b9ae3909-bea0-5146-8a0a-f7cf869026a7",
        "spec_version": "2.1",
        "revoked": false,
        "confidence": 75,
        "created": "2023-08-29T15:05:40.713Z",
        "modified": "2023-08-29T15:07:30.574Z",
        "name": "Dware-alt",
        "description": "Variant of the Dware malware",
        "malware_types": [
            "remote-access-trojan"
        ],
        "is_family": false,
        "last_seen": "2023-03-14T08:44:00.000Z",
        "capabilities": [
```

```
                "accesses-remote-machines"
            ],
            "kill_chain_phases": [
                {
                    "kill_chain_name": "mandiant-attack-lifecycle-model",
                    "phase_name": "escalate-privileges",
                    "x_opencti_order": 0
                }
            ],
            "x_opencti_id": "242be10f-a796-4612-a305-e41c5607f185",
            "x_opencti_type": "Malware",
            "type": "malware"
        },
        "threat-actor--3451f6c6-f512-5c53-956b-1c3cd5c7b06b": {
            "id": "threat-actor--3451f6c6-f512-5c53-956b-1c3cd5c7b06b",
            "spec_version": "2.1",
            "revoked": false,
            "confidence": 75,
            "created": "2023-08-16T13:08:56.115Z",
            "modified": "2023-08-16T13:16:10.407Z",
            "name": "RDMTA101",
            "threat_actor_types": [
                "spy"
            ],
            "first_seen": "2023-07-14T23:14:00.000Z",
            "last_seen": "2023-08-01T09:49:00.000Z",
            "roles": [
                "malware-author"
            ],
            "goals": [
                "RDMTA101 has been identified as a group of cyber- criminals tied with the
set. They are known for having authored several malware, in particular used for data exfil
            ],
            "sophistication": "expert",
            "resource_level": "government",
            "primary_motivation": "organizational-gain",
            "secondary_motivations": [
                "dominance"
            ],
            "personal_motivations": [
```

```
            "notoriety"
        ],
        "x_opencti_type": "Threat-Actor-Group",
        "threat_actor_group": "RDMTA101",
        "x_opencti_id": "56a1926c-9f0d-4e24-b62f-4ceae125f71c",
        "type": "threat-actor"
    },
    "vulnerability--c1349052-4b3d-53de-9393-dab76dd01052": {
        "id": "vulnerability--c1349052-4b3d-53de-9393-dab76dd01052",
        "spec_version": "2.1",
        "revoked": false,
        "confidence": 75,
        "created": "2023-08-16T13:47:42.563Z",
        "modified": "2023-08-16T13:47:42.599Z",
        "name": "CVE-2023-1477",
        "description": "Improper Authentication vulnerability in HYPR Keycloak Authen
        "x_opencti_base_score": 8,
        "x_opencti_base_severity": "HIGH",
        "x_opencti_attack_vector": "NETWORK",
        "external_references": [
            {
                "source_name": "CVE-2023-1477",
                "url": "https://nvd.nist.gov/vuln/detail/CVE-2023-1477",
                "external_id": "CVE-2023-1477"
            }
        ],
        "x_opencti_id": "99e4270d-6098-4105-862a-ceb43d552402",
        "x_opencti_type": "Vulnerability",
        "type": "vulnerability"
    }
}
```