Reference Incident Classification Taxonomy

Task Force Status and Way Forward

JANUARY 2018

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries in relation to this paper, please use CSIRT-Relations@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

- Members of Reference incident classification taxonomy task force (See Annex A)

Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

Table of Contents

1 Introduction 4
2 Background 5
2.1 Past work on Taxonomies 5
2.2 Trigger for Task Force 6
3 Task Force 7
3.1 Aim and Objectives 7
3.1.1 Upcoming Tasks 7
3.2 First Task Force Meeting 7
3.3 Current Members 8
4 Reference Incident Classification Taxonomy 9
4.1 Starting Point – ecsirt.net taxonomy 9
4.2 Sources 11
4.3 Correlation between Reference Taxonomy and Common Taxonomy for LE and CSIRTs 12
4.4 Mapping other Taxonomies 14
4.5 Pivot Mapping 15
4.6 MISP mapping 16
5. Conclusion 18
Annex A: Reference Incident Classification Taxonomy Member List 19

1 Introduction

Over the past years there have been several discussions around the topic of security incident classification taxonomies. A number of initiatives even resulted in new or modified taxonomies, such as the 'Common Taxonomy for (LE) Law Enforcement and CSIRTs,[1] which was set up to simplify CSIRT and LEA cooperation. This taxonomy resulted from collaboration initiatives such as the annual ENISA/EC3 Workshop which involved CSIRTs, LEAs, ENISA, and EC3. Other examples include the eCSIRT.net taxonomy[2] which was developed in 2003, and the eCSIRT.net mkVI taxonomy[3] which is an adaptation of the original eCSIRT.net taxonomy.

Creating a taxonomy is not a simple task. When dealing with topics like security incidents, there can be different ways in which to classify incidents, and it is not always easy or possible to determine which the best or correct classification is. Organisations defining a taxonomy are usually driven by different needs, and since different CSIRTs have different expectations, teams often end up developing their own incident classifications for internal use. In fact, the 'Common Taxonomy for LE and CSIRTs' is itself an adaptation of the CERT.PT taxonomy[4], which is itself an adaptation of the eCSIRT.net mkVI taxonomy. One main advantage of the Common Taxonomy for LE and CSIRTs for its use in the context of law enforcement is that it has been extended to also include a mapping of the incident classifications with a legal framework. Similarly, there have been a number of taxonomies that are in essence a branch or modification of another[5].

As the need for information exchange, and incident reporting increases, not to mention an increase in the use of automation in incident response, it is becoming evident that there is a need for common ground. This common ground would assist incident handlers dealing with technical incidents on a daily basis to deal with the abovementioned needs. Moreover, it could assist policy decision makers by offering a single reference point for discussing and drafting relevant policies such as the EU cyber security strategy and The Directive on security of network and information systems (NIS Directive). Following a discussion amongst the CSIRT community during the 51st TF-CSIRT meeting [6](15 May 2017 in The Hague, Netherlands), it was concluded that there is an urgent need for a taxonomy list and name everyone could rely on and refer to. This is where the Reference Incident Classification Taxonomy Task Force comes into play.

[1] https://www.europol.europa.eu/sites/default/files/documents/common_taxonomy_for_the_national_network_of_csirts.pdf
[2] http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html#HEAD6
[3] https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf
[4] https://www.cncs.gov.pt/certpt/
[5] https://github.com/MISP/misp-taxonomies
[6] https://tf-csirt.org/tf-csirt/meetings/51st-meeting/

2 Background

2.1 Past work on Taxonomies

ENISA has recently published two reports related to Incident Taxonomies:

- ENISA Report: Information sharing and common taxonomies between CSIRTs and Law Enforcement (Dec 2015) https://www.enisa.europa.eu/publications/information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement/at_download/fullReport
- ENISA Report: A good practice guide of using taxonomies in incident prevention and detection (Dec 2016) https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection/at_download/fullReport

In the first report, the main objective was to enhance cooperation both between the Member States (MS) of the EU and between related Network and Information Security (NIS) communities. It aimed at collecting and presenting information on projects facilitating information sharing between Member States CSIRTs and Law Enforcement. It also aimed at investigating which information can be shared between CSIRTs and Law Enforcement and how this can be achieved technically and organisationally. The following are some of the relevant proposals provided in this report:

- (to select) A taxonomy for the exchange of information based on desk research and based on the approval of the majority of the community.
- (to define) An update model for the taxonomy, to answer new requirements that could arise from the CSIRTs and the LEAs.
- (to develop) A roadmap for the implementation of the taxonomy in the exchange of information across CSIRTs and LEAs and the potential use of a sharing mechanism.

As an outcome of the report, a taxonomy was chosen as the best fitted to act as the nexus between LEAs and CSIRTs communities.

In the second report, the main objective was to provide relevant good practices in terms of taxonomies for incident detection and prevention for the CSIRT community. Additionally, it also provides conclusions and recommendations based on the qualitative assessment of taxonomies within the current taxonomy landscape on improvements that can be made on current taxonomies, such as what fields can be extended or added to existing taxonomies. Among the conclusions were the following:

- **A centralised repository for hosting all relevant taxonomies along with their versions should be set up by ENISA.**
- **A small set of common taxonomies for specific use cases should be agreed upon by CSIRTs at the EU level.**
- An “Other” or “Unknown”, “Tag” field should be used by the owners of taxonomies as an indicator to revise taxonomies, if there is an increase in that category with incidents or events of the same type.
- A roadmap towards standardised exchange formats in the CSIRTs community should be established at the EU level by the CSIRTs Network.

2.2 Trigger for Task Force

During the “51st TF-CSIRT meeting” (15 May 2017 in The Hague, Netherlands), members of the CSIRT community discussed the following points (amongst others):

- **There are two prominent taxonomies in the CSIRT community: “Common Taxonomy for Law Enforcement and CSIRTs”, and “eCSIRT.net mkVI”.**
- MISP[7] caters for “Common Taxonomy for Law Enforcement and CSIRTs”, while IntelMQ caters for the general categories.
- 11 categories are fixed, whilst the incident types (2nd column) is usually customised differently by teams.
- This topic cannot be decided by TF-CSIRT alone, it has to be coordinated with EC3, standardization would be a solution.
- **The general conclusion – There is the need for a taxonomy list and name everyone could rely on and refer to.**
- ENISA will set up a Task Force in this regard.

[7] MISP – Malware Information Sharing Platform - Open Source Threat Intelligence Platform & Open Standards for Threat Information Sharing

3 Task Force

3.1 Aim and Objectives

As mentioned in the 51st TF-CSIRT meeting, "there is the need for a taxonomy list and name everyone could rely on and refer to". As the need for information exchange, and incident reporting increases, not to mention an increase in the use of automation in incident response, it is becoming evident that there is need for some common ground. This common ground would assist incident handlers dealing with technical incidents on a daily basis to deal with the abovementioned needs. The aim of this task force is to enable the CSIRT community in reaching a consensus on a reference taxonomy. It should be noted that details such as identifying suitable sharing mechanisms are outside of the current scope. The objectives of the task force are the following:

- Develop Reference Document (Classifications, incident types or examples, and definition) using eCSIRT.net as a starting point.
- Define and develop an Update and Versioning Mechanism
- Host reference document
- Organise regular physical meetings with the stakeholders
- In the 2nd phase broader working group with non-European teams (FIRST) to achieve global consensus on incident reference taxonomy

3.1.1 Upcoming Tasks

The next meeting will be during the "53rd TF-CSIRT meeting" [8](5-7 February 2018 co-located with FIRST in Hamburg, Germany). Below are some of the tasks that need to be addressed by the task force.

- Decide on two elemental points
  - Use eCSIRT.net as starting point
  - Decide whether to focus on Incident Type or incident Example in the second column
- Review and consolidate Incident Classifications and definitions in the reference taxonomy (starting with eCSIRT.net)
- Define update workflow and Versioning Mechanism
- Decide about who will be Hosting online reference taxonomy (ENISA/Dedicated site, etc.)
- Propose way forward, e.g.: to meet periodically
- Decide on name (reference taxonomy/eCSIRT.net/other…)

3.2 First Task Force Meeting

Following the 51st TF-CSIRT meeting, a call for expression of interest for participation in the Reference Incident Classification Taxonomy Task Force was sent out via the TF-CSIRT mailing list, and the first task force meeting was set up back to back with the 52nd TF-CSIRT meeting (See Current Members below). Below are some of the discussion points and conclusions from this meeting:

- Different CSIRTs use their own taxonomy, or modified version of an existing eCSIRT.net taxonomy. A reference taxonomy will help us find a middle ground, even though CSIRTs will have their own implementation.

[8] https://first.org/events/symposium/hamburg2018/

- Reference Document (Classifications, types (and decision on their importance), and definition))
- Update and Versioning Mechanism.
- We need to decide on the hosting of the reference document.
- Following the upcoming meeting during TF-CSIRT in Hamburg, the reference taxonomy should be presented to other organisations such as FIRST[9] and ITF.
- There are differences in incident classification between CSIRTs and LEAs. However, they do go hand in hand and it is important to proceed accordingly.
- Fortunately, there are members that are both in the Reference Taxonomy task force, and the Taxonomy Governance Group of the CSIRT-LEA taxonomy which can ensure a harmonious evolution of the "Reference CSIRT incident Taxonomy" and the "Common Taxonomy for Law Enforcement and CSIRTs"
    - Mapping between the reference taxonomy and "Common Taxonomy for Law Enforcement and CSIRTs" is important
    - Consider including "Common Taxonomy for Law Enforcement and CSIRTs" with link to legal framework as an annex.
- It is important to define the objectives and outputs for the reference taxonomy (eg: statistics, information sharing and automation).
- Scope and Motivation
    - Taxonomy for CSIRT technical incidents
    - To ensure that CSIRTs are speaking the same language.
    - To facilitate sharing across CSIRTs.
    - To facilitate the harmonization of statistics between the CSIRT community.
    - To facilitate translation between different taxonomies, without disruption or need for major overhaul.
    - Could be useful mapping within the context of NIS directive
- The eCSIRT.net taxonomy seems to be a good starting point as a reference taxonomy.
- To discuss formal name of the new reference incident classification taxonomy.

3.3 Current Members

It is important that amongst the members of the task force are members of CSIRT teams, the Common Taxonomy Governance Group (including representatives from ENISA and EC3), tool developers (MISP/IntelMQ…), and taxonomy owners (owner of eCSIRT.net). A mailing list has been set up in order to facilitate communication between the task force members.

See Annex A for the current list of participants.

[9] FIRST - the global Forum of Incident Response and Security Teams

4 Reference Incident Classification Taxonomy

To give a better understanding of how a reference taxonomy can benefit the community, we demonstrate a high level mapping of 4 taxonomies: eCSIRT.net (reference taxonomy), Common Taxonomy for LE and CSIRTs, and two CSIRT provided taxonomies (CIRCL.LU and CERT.LV).

4.1 Starting Point – ecsirt.net taxonomy

The main action item following the first task force meeting was to determine whether the eCSIRT.net taxonomy was a suitable candidate as a starting point for the reference taxonomy. The official latest version is the eCSIRT.net mkVI:

INCIDENT CLASSIFICATION	INCIDENT EXAMPLES	DESCRIPTION
Abusive Content	Spam	or "Unsolicited Bulk Email", this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a functionally comparable content
	Harmful Speech	Discreditation or discrimination of somebody (e.g. cyber stalking, racism and threats against one or more individuals)
	Child/Sexual/Violence/ ...	Child pornography, glorification of violence, ...
Malicious Code	Virus	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
	Worm	
	Trojan	
	Spyware	
	Dialler	
	Rootkit	
Information Gathering	Scanning	Attacks that send requests to a system to discover weak points. This includes also some kind of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, …), port scanning.
	Sniffing	Observing and recording of network traffic (wiretapping).
	Social engineering	Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).
Intrusion Attempts	Exploiting known vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (e.g. buffer overflow, backdoor, cross site scripting, etc.).
	Login attempts	Multiple login attempts (Guessing / cracking of passwords, brute force).
	New attack signature	An attempt using an unknown exploit.
Intrusions	Privileged account compromise	A successful compromise of a system or application (service). This can have been caused remotely by a known or new vulnerability, but also by an unauthorized local access. Also includes being part of a botnet.
	Unprivileged account compromise	

	Application compromise Bot	
Availability	DoS DDoS Sabotage Outage (no malice)	By this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. DoS examples are ICMP and SYN floods, Teardrop attacks and mail-bombing. DDoS often is based on DoS attacks originating from botnets, but also other scenarios exist like DNS Amplification attacks. However, the availability also can be affected by local actions (destruction, disruption of power supply, etc.) – or by Act of God, spontaneous failures or human error, without malice or gross neglect being involved.
Information Content Security	Unauthorised access to information Unauthorised modification of information	Besides a local abuse of data and systems the information security can be endangered by a successful account or application compromise. Furthermore, attacks are possible that intercept and access information during transmission (wiretapping, spoofing or hijacking). Human/configuration/software error can also be the cause.
Fraud	Unauthorized use of resources	Using resources for unauthorized purposes including profit-making ventures (E.g. the use of e-mail to participate in illegal profit chain letters or pyramid schemes).
	Copyright	Offering or Installing copies of unlicensed commercial software or other copyright protected materials (Warez).
	Masquerade	Type of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it.
	Phishing	Masquerading as another entity in order to persuade the user to reveal a private credential.
Vulnerable	Open for abuse	Open resolvers, world readable printers, vulnerability apparent from Nessus etc scans, virus signatures not up-to-date, etc
Other	All incidents which do not fit in one of the given categories should be put into this class.	If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised.
Test	Meant for testing	Meant for testing

Table 1: eCSIRT.net mkVI

This is not necessarily an ideal taxonomy. However, it has many factors which make it very useful. In particular, the main categories seem to be very practical and universal. Even though the taxonomy was developed many years ago (and has gone over a number of adaptations), the main categories are still current and can easily be used today. The same cannot be said about the subcategories which can sometimes lead to problems with how to classify an incident. For example, it is not particularly useful any more to make a distinction between DoS attacks and DDoS attacks or to determine what is a ’privileged account compromise’, ’unprivileged account compromise’ or ’application compromise’. In practice, subcategories became a part of the description rather than a concrete schema for classification. Nowadays it is really difficult to determine if a particular malware is a virus, worm, Trojan, spyware or a dialler. The functionality of malware changes and the honest approach is to classify it all as ‘malicious code’.

The eCSIRT.net classification is highly recommended. Despite some defects, it is still quite useful and good. Many European CSIRTs use it, which will give teams the opportunity to team up with others later and be able to compare and merge statistics.

4.2 Sources

During the 51st TF-CSIRT meeting, one of the main conclusions was that there is the need for a taxonomy list and name everyone could rely on and refer to. When one considers the eCSIRT.net taxonomy, there currently exist different sources where the taxonomy is hosted:

Trusted Introducer (Official document):

- https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf

ENISA's page:

- https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies

MISP documentation and Github page:

- https://github.com/MISP/misp-taxonomies/blob/master/ecsirt/machinetag.json
- http://www.misp-project.org/taxonomies.html#_ecsirt
- https://www.misp-project.org/taxonomies.pdf

IntelMQ:

- http://intelmq.readthedocs.io/en/latest/Data-Harmonization/

4.3 Correlation between Reference Taxonomy and Common Taxonomy for LE and CSIRTs

An advantage of the Reference Taxonomy is its tight correlation with the Common Taxonomy for LE and CSIRTs, which is itself an adaptation of the CERT.PT taxonomy, which is an adaptation of the eCSIRT.net mkVI. Here we will see a high level mapping of eCSIRT.net to the Common Taxonomy for Law Enforcement and CSIRTs.

REFERENCE TAXONOMY (ECSIRT.NET)[10]	COMMON TAXONOMY FOR LE AND CSIRTS	NOTE
Abusive Content	**Abusive Content**	
Malicious Code	**Malware**	
Information Gathering	**Information Gathering**	
Intrusion Attempts	**Intrusion Attempts**	
Intrusion	**Intrusion**	
Availability	**Availability**	
Information Content Security	**Information Security**	
Fraud	**Fraud**	
Vulnerable	⬛	Not relevant to LEA
Other	**Other**	
Test	⬛	Not relevant to LEA

Table 2: Reference taxonomy vs Common Taxonomy for LE and CSIRTs

LEGEND	
🟩	The same
🟥	Not mentioned in the other taxonomy
⬛	Not present

Table 3 shows a very close correlation between the Reference Taxonomy, and the Common Taxonomy for LE and CSIRTs with regards to the main categories (first column). In fact, there is almost a one-to-one mapping of the existing categories in both taxonomies. However, this is not the case for the incident type and examples (second column).

[10] The term 'Reference taxonomy' will be used to refer to the eCSIRT.net

REFERENCE TAXONOMY INCIDENT CLASSIFICATION (1ST COLUMN)	INCIDENT EXAMPLES (2ND COLUMN)
Abusive Content	🟩 Spam
	🟧 Harmful Speech
	🟧 Child/Sexual/Violence/...
Malicious Code	🟧 Virus
	🟧 Worm
	🟧 Trojan
	🟧 Spyware
	🟧 Dialler
	🟧 Rootkit
Information Gathering	🟩 Scanning
	🟩 Sniffing
	🟧 Social engineering
Intrusion Attempts	🟩 Exploiting known vulnerabilities
	🟩 Login attempts
	🟥 New attack signature
Intrusions	🟧 Privileged account compromise
	🟧 Unprivileged account compromise
	🟧 Application compromise
	🟥 Bot
Availability	🟧 DoS
	🟧 DDoS
	🟩 Sabotage
	🟥 Outage (no malice)
Information Content Security	🟩 Unauthorised access to information
	🟩 Unauthorised modification of info
Fraud	🟩 Unauthorized use of resources
	🟦 Copyright
	🟧 Masquerade
	🟦 Phishing
🟥 **Vulnerable**	🟥 Open for abuse
Other	🟩 Other
🟥 **Test**	🟥 Meant for testing

INCIDENT TYPE (2ND COLUMN)	COMMON TAXONOMY FOR LE AND CSIRTSINCIDENT CLASSIFICATION (1ST COLUMN)
🟩 SPAM	**Abusive Content**
🟦 Copyright	
🟧 Child Sexual Exploitation, racism and incitement to violence	
🟧 Infection	**Malware**
🟧 Distribution	
🟥 C&C	
🟥 Undetermined	
🟥 Malicious Connection	
🟩 Scanning	**Information Gathering**
🟩 Sniffing	
🟦 Phishing	
🟩 Exploitation of vulnerability	**Intrusion Attempts**
🟩 Login attempt	
🟧 (Successful) Exploitation of vulnerability	**Intrusion**
🟧 Compromising an account	
🟧 DoS/DDoS	**Availability**
🟩 Sabotage	
🟩 Unauthorised access	**Information Security**
🟩 Unauthorised modification/deletion	
🟩 Misuse or unauthorised use of resources	**Fraud**
🟧 False representation	
🟧 Unlisted incident	**Other**
🟧 Undetermined incident	

LEGEND	
🟩	The same
🟧	Similar but with some differences
🟦	The same but in a different category
🟥	Not mentioned in the other taxonomy

Table 3: Detailed Reference taxonomy vs Common Taxonomy for LE and CSIRTs

Consider the side-by-side comparison above. It outlines the differences in the “Incident Example” in the Reference Taxonomy, and “Incident Type” in the Common Taxonomy for LE and CSIRTs. Moreover, the Common Taxonomy for LE and CSIRTs also includes a third column which includes the link to the legal framework. This is not always directly relevant to the CSIRT community, however, it could very be useful especially when cooperating with law enforcement. The mapping between these two taxonomies could help to identify factors that could lead to the update or inclusion of new incident types. Consider for example the incident types for the malware category of both the Reference Taxonomy, and Common taxonomy for LE and CSIRTs. There are significant differences between the two, where the Reference Taxonomy focuses more on the technical specification of the malware type, and the Common taxonomy for LE and CSIRTs distinguishes between infection and distribution. This does not seem to be considered in the Reference Taxonomy. The task force could use these kinds of differences to determine whether or not such incident types should be added to the reference taxonomy.

REFERENCE TAXONOMY INCIDENT CLASSIFICATION (1ST COLUMN)	INCIDENT EXAMPLES (2ND COLUMN)
Malicious Code	Virus
	Worm
	Trojan
	Spyware
	Dialler
	Rootkit

INCIDENT TYPE (2ND COLUMN)	COMMON TAXONOMY FOR LEA AND CSIRT INCIDENT CLASSIFICATION (1ST COLUMN)
Infection	Malware
Distribution	
C&C	
Undetermined	
Malicious Connection	

4.4 Mapping other Taxonomies

As mentioned earlier, the Reference taxonomy contains a very practical and universal high level categorisation. Below are examples of existing taxonomies (CERT.LV[11], and CIRCL.LU[12]), demonstrating how most of their high level categories map into one or more categories from the Reference Taxonomy. In the case of CERT.LV, there is a clear one-to-one mapping with all (except testing) of the high level categories. However, the mapping between CIRCL.LU and Reference Taxonomy is not as direct.

[11] https://cert.lv/en/incidents

[12] https://github.com/MISP/misp-taxonomies/blob/master/circl/machinetag.json

REFERENCE TAXONOMY	CERT.LV TAXONOMY
Abusive Content	Abusive Content
Malicious Code	Malicious Code
Information Gathering	Information Gathering
Intrusion Attempts	Intrusion Attempts
Intrusion	Intrusion
Availability	Availability
Information Content Security	Information Content Security
Fraud	Fraud
Vulnerable	Vulnerable
Other	Other
Test	

Table 4: Reference Taxonomy vs CERT.LV taxonomy

CIRCL TAXONOMY	REFERENCE TAXONOMY
Spam	Abusive Content
malware	Malicious Code
Scan	Information Gathering
	Intrusion Attempts
system-compromise	Intrusions
XSS	
sql-injection	
denial-of-service	Availability
information-leak	Information Content Security
copyright-issue	Fraud
phishing,	
Scam	
vulnerability	Vulnerable
Fastflux	Other
	Test

Table 5: CIRCL taxonomy vs Reference Taxonomy

4.5 Pivot Mapping

Given the tight correlation between the Reference Taxonomy and a number of other taxonomies such as the Common Taxonomy for LE and CSIRTs, a mapping from a particular taxonomy to the Reference Taxonomy, automatically generates a mapping between that taxonomy and other previously mapped taxonomies. Consider the following example of how CIRCL.LU taxonomy can be mapped to the Common Taxonomy for LE and CSIRTs and the CERT.LV taxonomy by pivoting from one taxonomy to another.

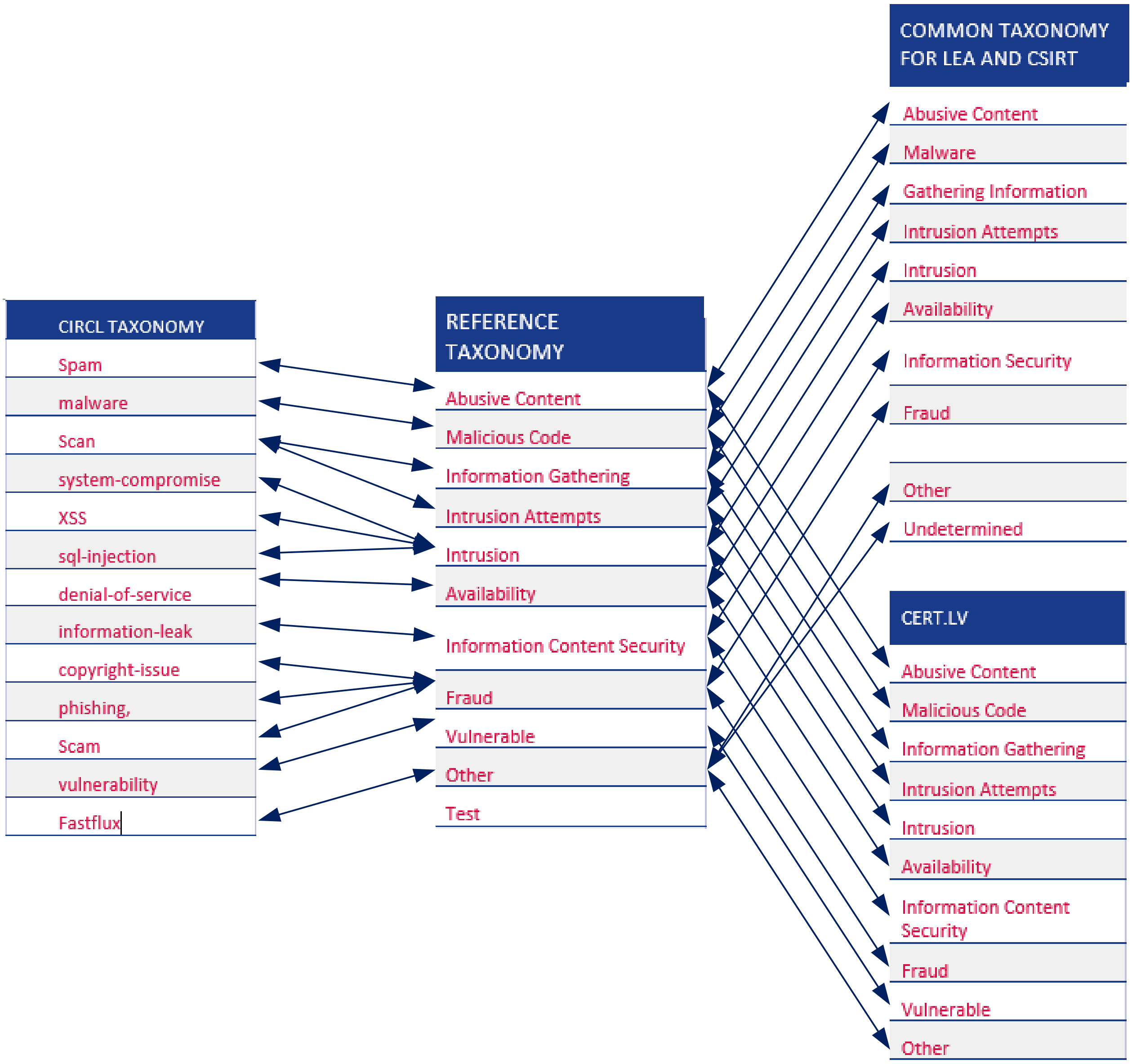


Figure 1: Pivot Mapping

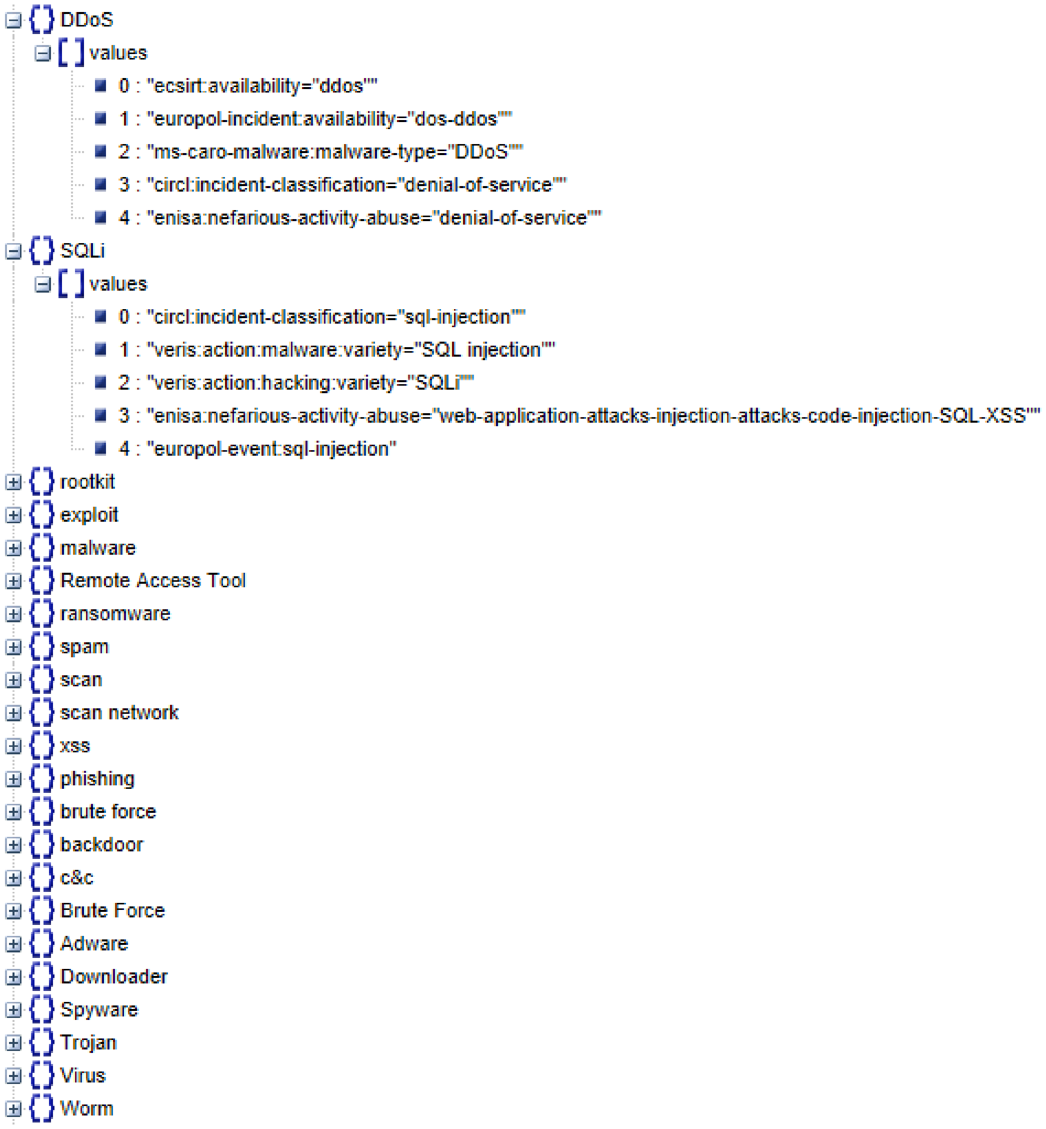
Notice that since both the Common Taxonomy for LE and CSIRTs, and CERT.LV Taxonomy have been mapped onto the Reference Taxonomy, this provides a clear mapping between the Common Taxonomy for LE and CSIRTs and the CERT.LV taxonomy, as well as any other taxonomy that would have already been mapped to the Reference Taxonomy. This mapping can be extremely useful for cross-CSIRT collaboration, as well as CSIRT-LEA collaboration by enabling CSIRTs to use the Common Taxonomy for LE and CSIRTs.

4.6 MISP mapping

MISP developers have provided a mapping of existing taxonomies.

- https://github.com/MISP/misp-taxonomies/blob/master/mapping/mapping.json
- http://www.misp-project.org/taxonomies.html#_mapping_of_taxonomies

The MISP mapping taxonomy allows for the mapping of a single classification into a series of machine-tag synonyms. The implemented approach for mapping is similar to the one described above, whereby a number of categories are used as a central reference point and each of these points are mapped to categories in other known taxonomies.



```
⊟ { } DDoS
    ⊟ [ ] values
        ■ 0 : "ecsirt:availability="ddos""
        ■ 1 : "europol-incident:availability="dos-ddos""
        ■ 2 : "ms-caro-malware:malware-type="DDoS""
        ■ 3 : "circl:incident-classification="denial-of-service""
        ■ 4 : "enisa:nefarious-activity-abuse="denial-of-service""
⊟ { } SQLi
    ⊟ [ ] values
        ■ 0 : "circl:incident-classification="sql-injection""
        ■ 1 : "veris:action:malware:variety="SQL injection""
        ■ 2 : "veris:action:hacking:variety="SQLi""
        ■ 3 : "enisa:nefarious-activity-abuse="web-application-attacks-injection-attacks-code-injection-SQL-XSS""
        ■ 4 : "europol-event:sql-injection"
⊞ { } rootkit
⊞ { } exploit
⊞ { } malware
⊞ { } Remote Access Tool
⊞ { } ransomware
⊞ { } spam
⊞ { } scan
⊞ { } scan network
⊞ { } xss
⊞ { } phishing
⊞ { } brute force
⊞ { } backdoor
⊞ { } c&c
⊞ { } Brute Force
⊞ { } Adware
⊞ { } Downloader
⊞ { } Spyware
⊞ { } Trojan
⊞ { } Virus
⊞ { } Worm
```

Figure 2: JSON values of MISP mapping taxonomy

Figure 2 shows how the taxonomies are mapped in the MISP taxonomy document.

5. Conclusion

While still in its infancy, the reference taxonomy task force is off to a good start. The members seem eager and willing to contribute, and make use of the resulting reference taxonomy. The outcome of the upcoming meetings will determine the success of this initiative. In these meetings, the task force plans to:

- Decide on two elemental points
  - Confirm eCSIRT.net as starting point
  - Decide whether to focus on Incident Type or incident Example in the second column
- Review and consolidate Incident Classifications and definitions in the reference taxonomy (starting with eCSIRT.net)
- Define update workflow and Versioning Mechanism
- Decide about who will be hosting online reference taxonomy (ENISA/Dedicated site,etc.)
- Propose way forward, e.g.: to meet periodically
- Decide on name (reference taxonomy/eCSIRT.net/other…)

Annex A: Reference Incident Classification Taxonomy Member List

- Sebastien Schmitt (Gemalto)
- Jan Kopriva (ALEF-CSIRT)
- Toomas Lepik (Tallinn University)
- Sven Gabriel (EGI-CSIRT)
- Kris Caron (KBC Group CERT)
- Silvio Oertli (SWITCH CERT)
- Vladimir Bobor (Telia CERT)
- Bilgehan Turan (EATM-CERT)
- Vasileios Friligkos (EATM-CERT)
- David Alfós (CaixaBank)
- Marcolla, Sara Veronica (EC3)
- Azofra Martínez, Álvaro (EC3)
- Baiba Kaskina (CERT.LV/TF-CSIRT)
- Pavel Kácha (CESNET)
- Thomas Schreck (Siemens)
- L. Aaron Kaplan (CERT.AT)
- Michael Hamm (CIRCL.lu)
- Jean Paul Weber (GOVCERT.LU)
- MANA Patrick (Eurocontrol)
- Johannes Clos (BSI/CERT-Bund)
- Jonsson Robert (CERT-SE)
- Gorazd Božič (SI-CERT)
- Francisco Jesus Monserrat Coll. (IRIS-CERT)
- Klaus-Peter Kossakowski (DFN-CERT)
- Francesco Canestrelli (Open Systems)
- Rossella Mattioli (ENISA)
- Yonas Leguesse (ENISA)
- Andrea Dufkova (ENISA)
- Theodoros Nikolakopoulos (ENISA)
- Don Stikvoort (S-CURE)
- Alexandre Dulaunoy (CIRCL.lu)
- Lionel Ferette (CERT.be)
- Otmar Lendl (CERT.AT)
- Thomas Hungenberg (CERT-Bund)
- Sebastian Wagner (CERT.AT)
- Ian Bryant (UK MOD / University of Warwick)
- N/A (CCN-CERT)

ENISA
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu