

The Role of a Threat Observatory

Section Threat landscape

NISDUC Conference, Brussels

Day 1: Tuesday, April 25



Competence building



Capacity building



Research, data & innovation



Ecosystem & industrialization



NCC coordination

ABOUT US

The NC3 mission is to support the Luxembourg ecosystem in building cybersecurity competence and capacity, in a way that contributes to develop the cybersecurity industrial base, and strengthens the strategic autonomy of the European Union.

Objectives of the Observatory

The primary objective of the National Cybersecurity Competence Centre (NC3) is to assist enterprises (with a strong focus on SMEs) as well as NGO's and Municipalities. To this end, NC3 has created an observatory, the **Threat Observatory Platform (NC3 TOP)**, to monitor and report on cyber threats and risks.

NC3 TOP's primary purpose is to provide users with **reliable and factual information** about emerging threats to aid in their decision-making process. By doing so, it assists users in selecting the **best prevention strategies to pursue**, with a specific emphasis on optimizing the allocation of **security spending**.

Main sources of information



MISP is an open source threat intelligence platform for sharing, storing and correlating Indicators of Compromise (IoC's) of targeted attacks, threat intelligence, financial fraud information, or vulnerability information



SPAMBEE is a tool for handling suspicious emails. It conducts a comprehensive diagnosis of any suspicious email to determine whether it is spam or phishing.

Conceptual Model

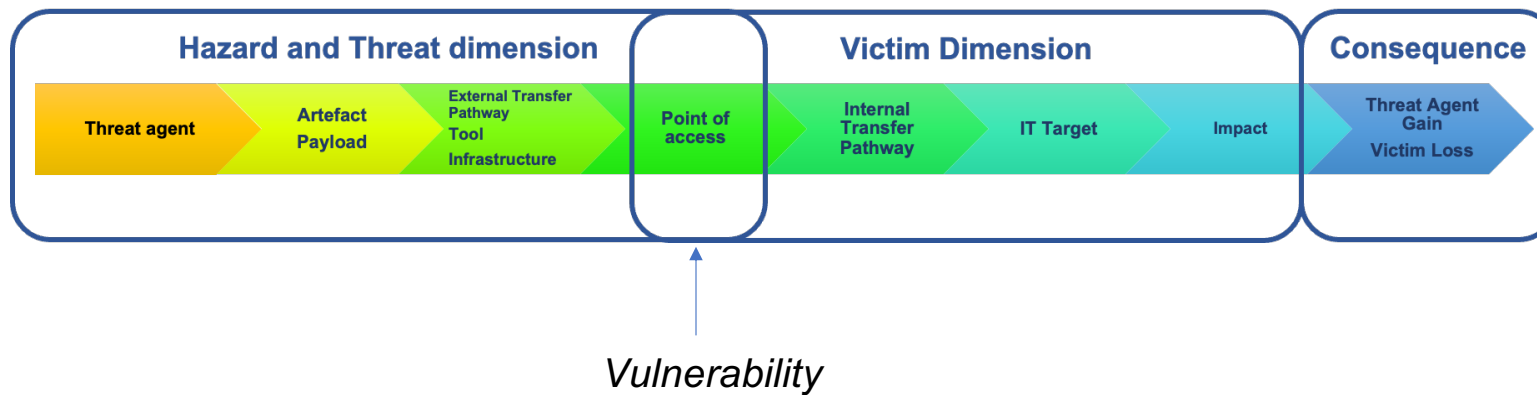
A simplified conceptual model was defined to enhance the utilization of cyber threat information by **non-experts**, eliminate the use of technical jargon, and adopt a strict interpretative method of risk assessment.

The primary objective was to improve the **accessibility and understanding** of cyber threat information for a **broader audience**.

Def.: $\text{Risk} = \text{Prob}(\text{Threat}) \otimes \text{Consequence}(\text{Vulnerability}(\text{Esposed Asset}))$

Conceptual Model

$$\text{Risk} = \text{Prob}(\text{Threat}) \otimes \text{Cosequence}(\text{Vulnerability}(\text{Exposed Asset}))$$



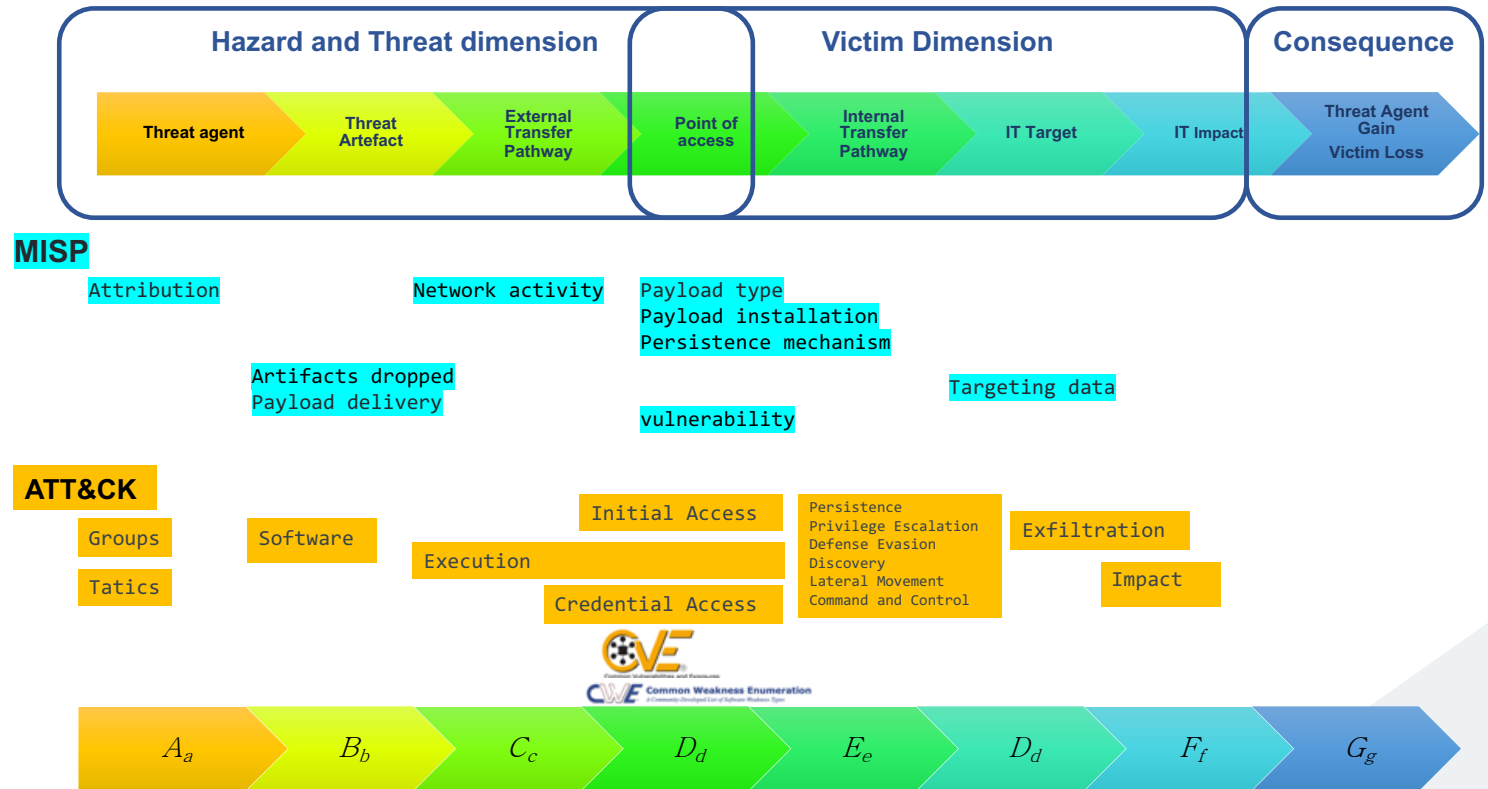
2 type of Consequence

All the different aspects are relevant for supporting the risk management process

Mapping the information

The proposed model allows interpreting the available MISP information.

The model also allows the integration of the MISP information with other sources.



Info Classification Process

Natural language processing techniques: The MISP & SPAMBEE records are subjected to natural language processing techniques, such as tokenization and Named Entity Recognition (NER), to extract valuable information and insights while also categorizing and organizing the data.

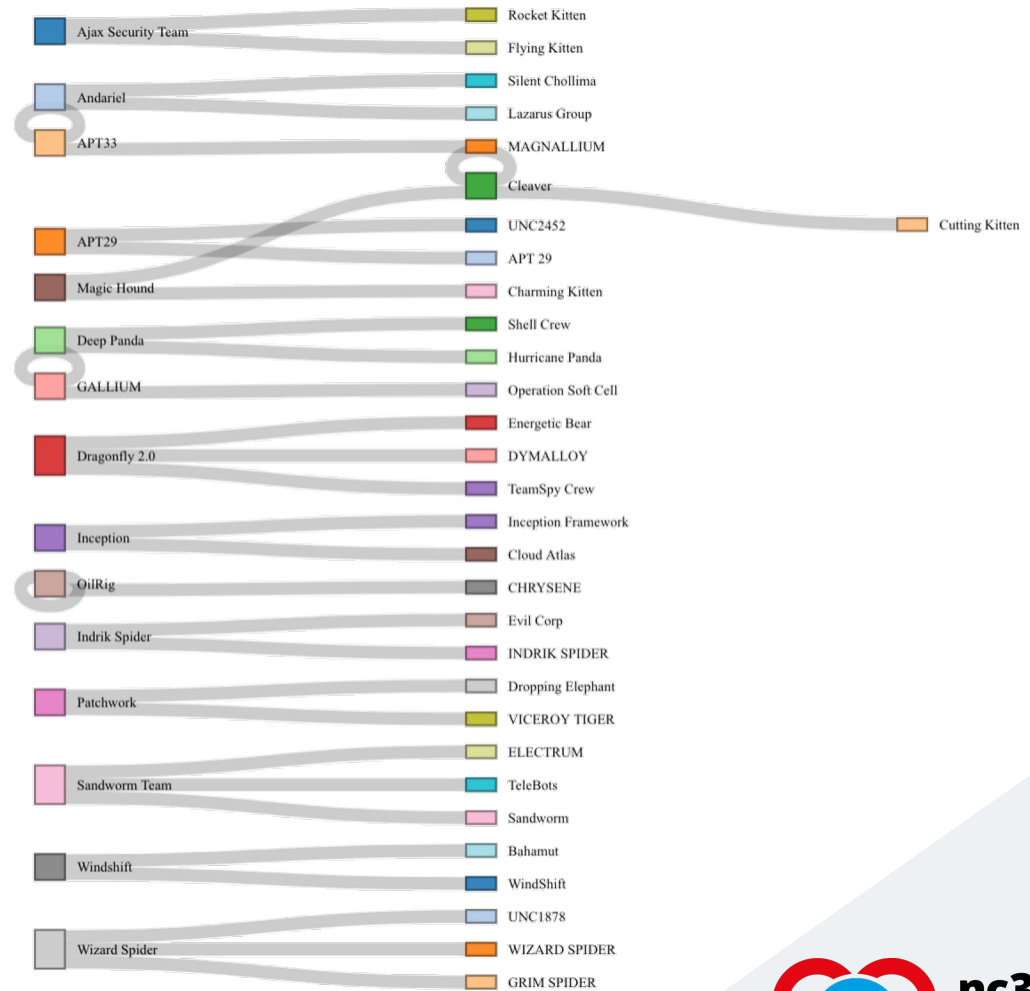
The mapping process involves scanning data records against reference information across all dimensions of the conceptual risk model. The reference information utilized is derived from reputable and established sources that are well-known and widely recognized.



These techniques help in identifying significant entities and breaking down the information into manageable segments for better understanding and analysis.

Example

Comparison of nomenclature of threat actors between MITRE ATT&CK® and MISP

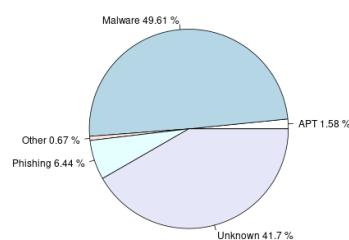


Simply monitoring & Counting?

Event types

Comparison of event types

Event distribution in 2020



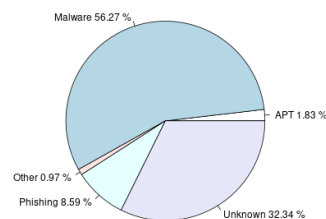
Details

Show **10** entries Search:

Type	Count	Percentage
1 APT	130	1.58 %
2 Malware	4069	49.61 %
3 Other	55	0.67 %
4 Phishing	528	6.44 %
5 Unknown	3420	41.7 %

Showing 1 to 5 of 5 entries Previous **1** Next

Event distribution in 2021



Details

Show **10** entries Search:

Type	Count	Percentage
1 APT	19	1.83 %
2 Malware	583	56.27 %
3 Other	10	0.97 %
4 Phishing	89	8.59 %
5 Unknown	335	32.34 %

Showing 1 to 5 of 5 entries Previous **1** Next

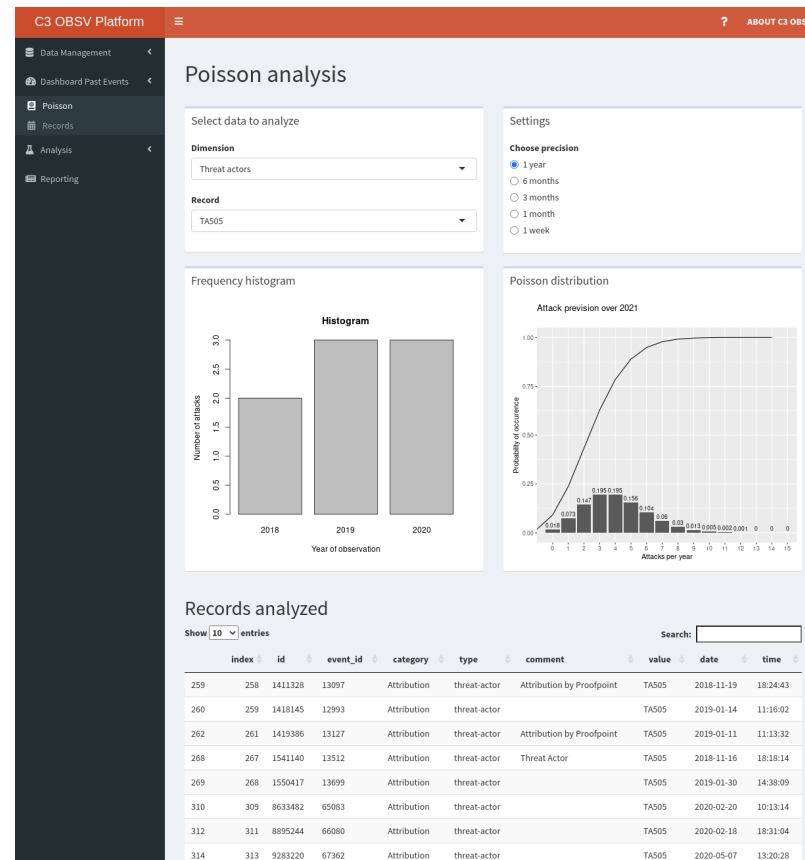
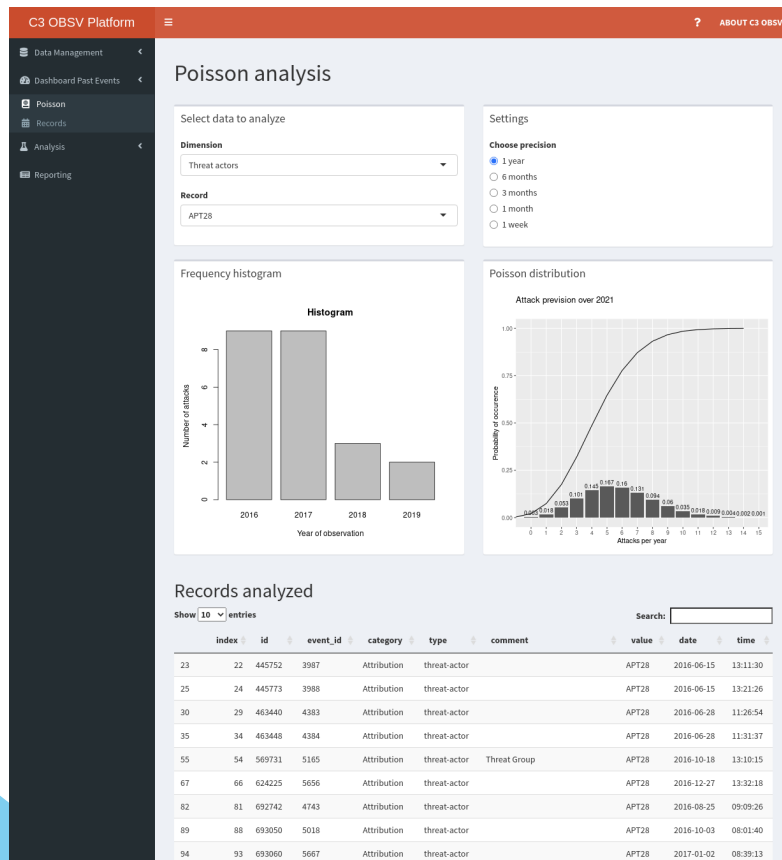
		Number	Event / Day	Event / Year	Rate
Malware	2020	4069	11,1	4.069,0	0,6
	1 Jan - 30 March 2021	583	6,5	2.364,4	
ATP	2020	130	0,36	130,0	0,6
	1 Jan - 30 March 2021	19	0,21	77,1	
Phishing	2020	528	1,4	528,0	0,7
	1 Jan - 30 March 2021	89	1,0	360,9	

More than simply counting

11

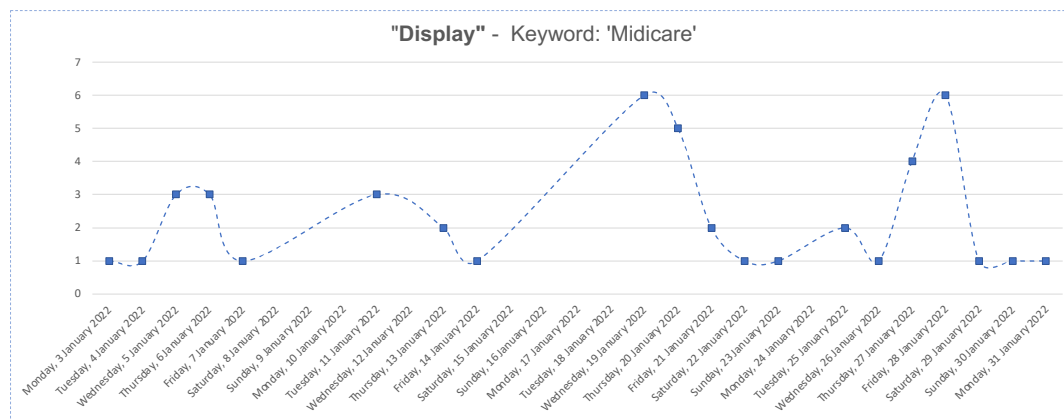
21-Apr-23

Interpretation of potential threat occurrence

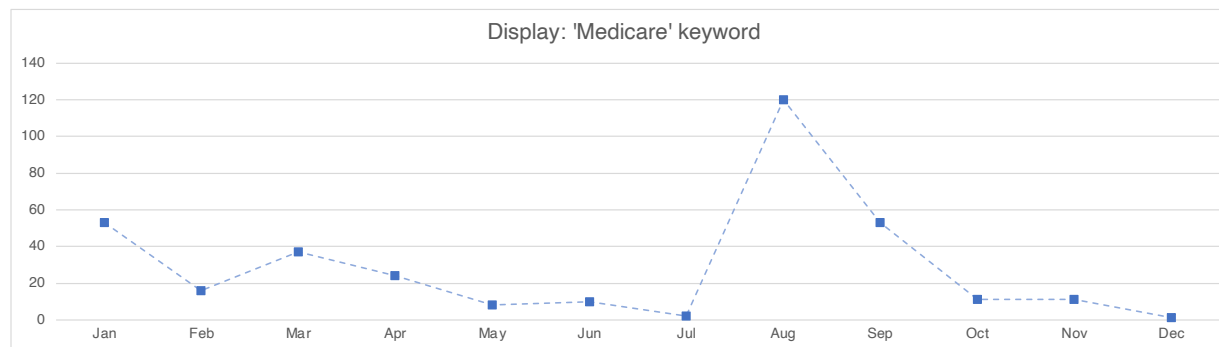


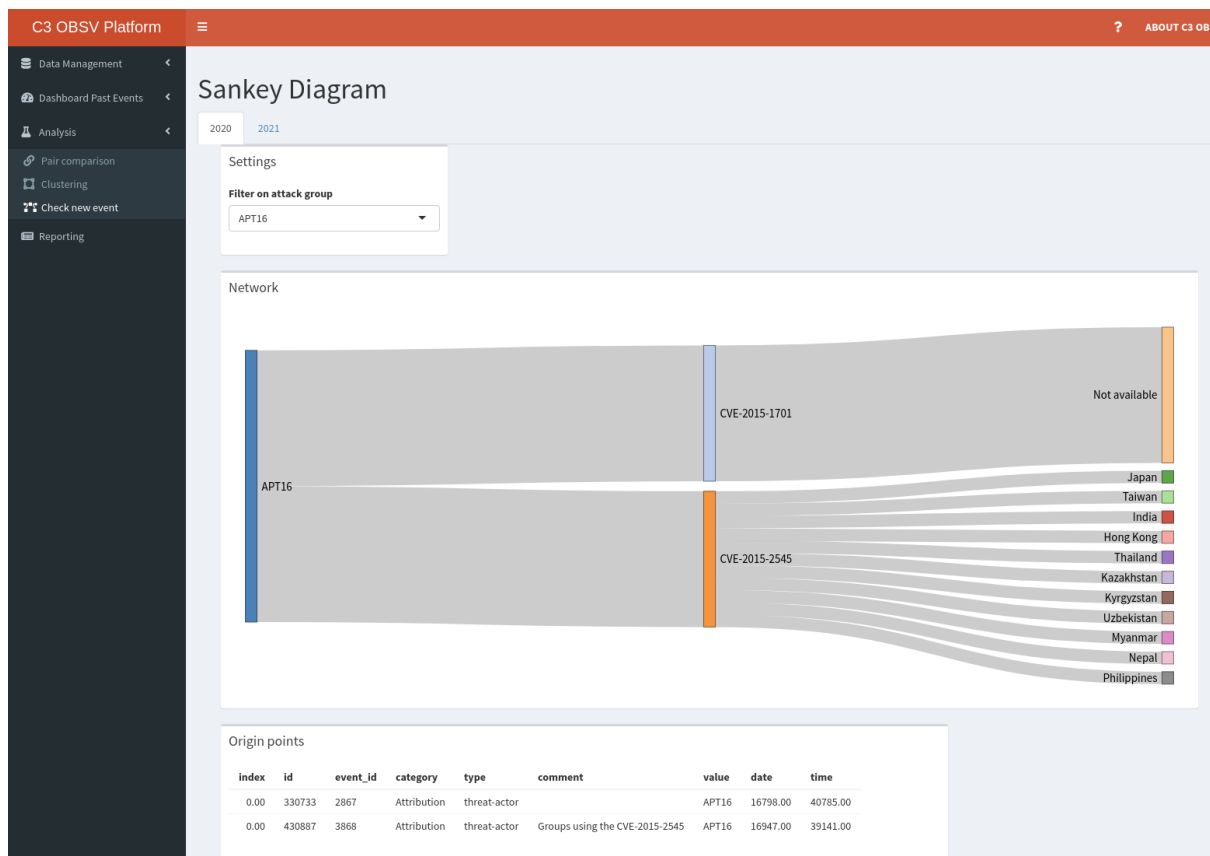
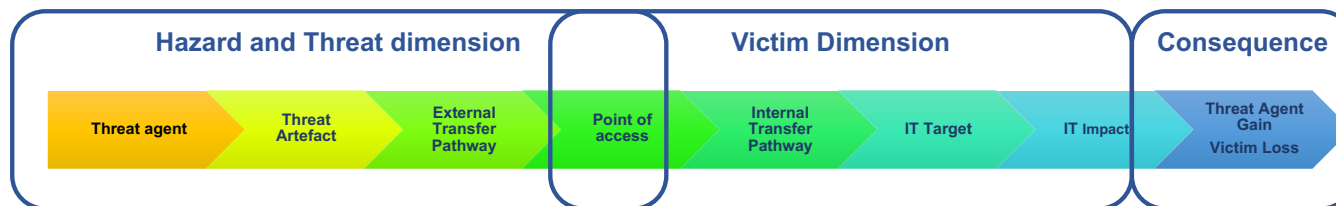
Phishing example

January 2022

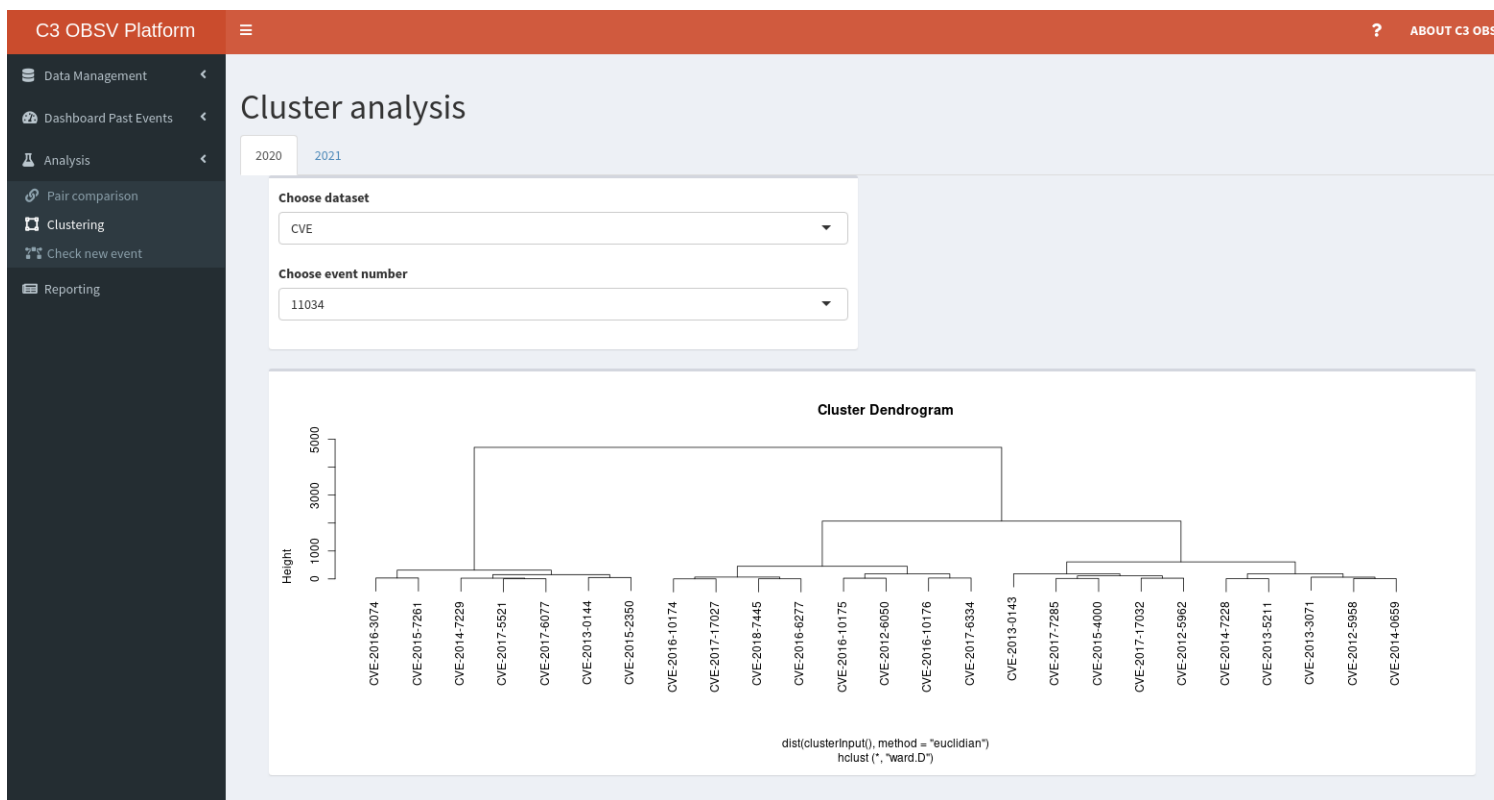


Year 2022





Previous Recorded CVEs - similarities

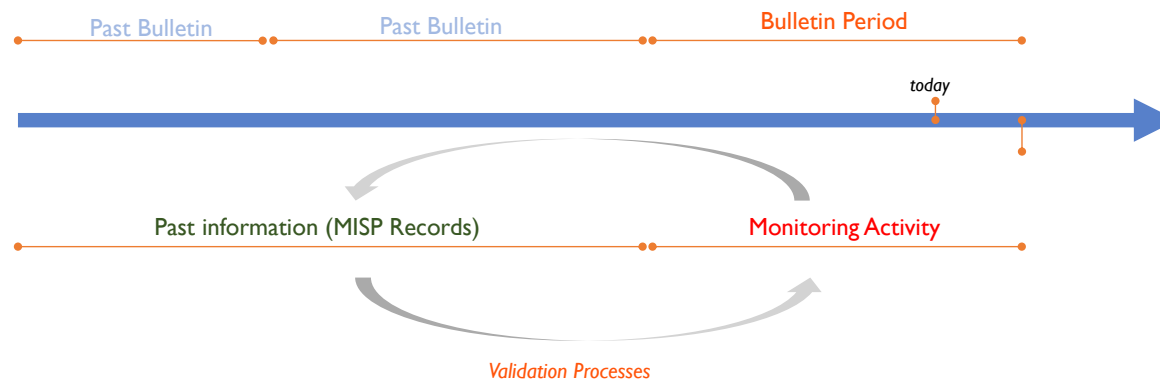


Dissemination

16



21-Apr-23

Dissemination strategy



Bulletin: type of information

1. Quarter of the year covered by the present Bulletin
2. Dimension of the model described in the table
3. Entities or items identified as the most prevalent during the Quarter covered by the Bulletin
4. Number of items and percentage relative to the total number of items in this category
5. Total number of attribute and unattributed items, where “attributed” means that the corresponding event can be linked with an item of the Dimension
6. Rate of attribution showing the proportion of events that can be attributed relatively to the overall number of events
7. comparison with the previous quarter and corresponding trend

 BULLETIN 						
1 Qtr2_2020						
2 THREAT ACTOR						
3		4 Qtr1_2020		Qtr2_2020		7 Trend
		#	%	#	%	
	APT41	3	0,11%	3	0,13%	→
	Gamaredon Group	4	0,15%	4	0,17%	→
	Lazarus Group	0	0,00%	3	0,13%	↑
	Turla	2	0,07%	6	0,26%	↑
5 Number of attributed events		61	2,23%	39	1,70%	▼
Number of unattributed events		2677	97,77%	2250	98,30%	▽
6 Attribution Rate		2,2%		1,7%		▽

Trend Legend	
↑	Increasing trend (worsening)
↗	Slight increasing trend (worsening)
→	Stable trend
↘	Slight decreasing trend (improvement)
↓	Decreasing trend (improvement)

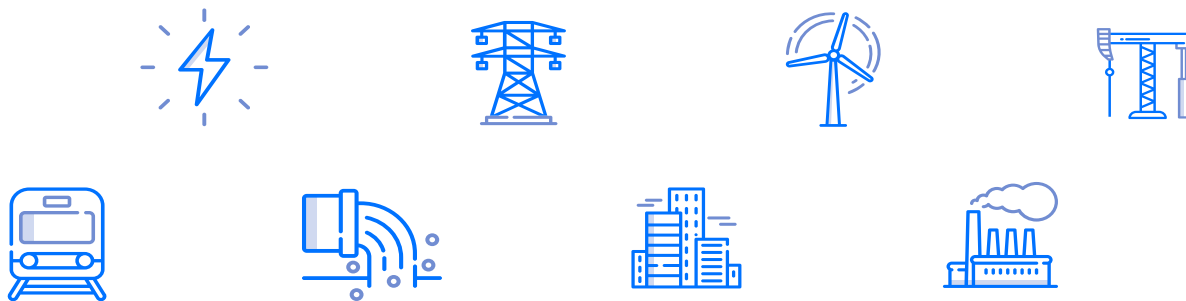
Attribution Rate Legend	
▼	Decreasing Attribution Rate
▽	Slight Decreasing Attribution Rate
=	Stable Attribution Rate
△	Slight Increasing Attribution Rate
▲	Increasing Attribution Rate


— Observatory & NIS2

NIS2 directive

Article 21 - NIS2 requires essential and important entities to take **appropriate measures** to manage cybersecurity risks and prevent or minimize the impact of incidents on their services and recipients of those services.

The **observatory's activities** help **companies** to implement the NIS2 and to protect economies and society.





The directive's impact assessment* indicates that companies falling under the NIS2 framework's scope would need to increase their current IT security spending by up to 22% during the first few years after the new NIS framework's introduction.

The observatory activities can help in containing such costs.

* <https://digital-strategy.ec.europa.eu/en/library/impact-assessment-proposal-directive-measures-high-common-level-cybersecurity-across-union>

NIS2 implementation

Observatory support

NIS2 places a particular responsibility on the management bodies of essential and important entities to approve and oversee the implementation of cybersecurity risk management measures, and it holds them liable for failing to do so.

The Observatory can help operators:

- To define and to review cyber security policies;
- To define appropriate operational, organizational and technical measures.
- To define and to maintain a cyber security roadmap;
- To design and review the business continuity plan (risk analyses, BIA, security awareness and incident management)
- On situational awareness



Conclusions

The activities conducted by the observatory can assist in **mitigating costs**.

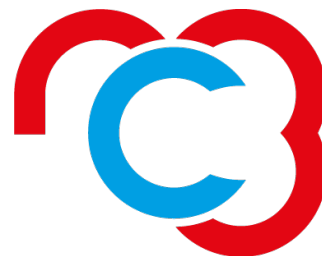
By providing users with up-to-date and accurate information on emerging threats, the observatory can aid in the **development and implementation of effective prevention strategies**.

This can help companies **avoid costly** security breaches and reduce the financial impact of potential cyber attacks.

The observatory's activities can also help companies make **informed decisions** on security spending, ensuring that resources are **allocated effectively** to address the most critical cybersecurity risks.

THANK YOU FOR YOUR ATTENTION

C. Dimauro
carmelo.dimauro@nc3.lu



nc3.lu

National Cybersecurity
Competence Center
LUXEMBOURG



**122, rue Adolphe Fischer
L-1521 Luxembourg**



+352 274 00 98 667



info@nc3.lu



<https://nc3.lu>