InCyber Forum
02/04/2025

Preventing and Mitigating Cyber Risks in Electric Infrastructures

S2 Grupo / Sergio Villanueva Tolosa

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. Horizon Europe Grant agreement N° 101075714.

Reliability, Resilience and Defense technology for the grid

S2 Grupo in numbers

S2GRUPO
Anticipando un mundo ciberseguro

Over
20 years
of cyber security experience

More tan
10 certifications

700+ cybersecurity experts

+1000 Customers
trust us:
- 75% IBEX35 customers
- Multilateral organisations
- All sectors

50 R&D&I projects
with more than 10% of our turnover invested each year

Operations in
more than 35 countries

Offices in Spain, Rotterdam, Portugal, Colombia and Chile

Proprietary
protection and detection technologies

Proprietary and shared tools
with CCN CERT
- GLORIA
- CARMEN
- CLAUDIA
- MICROCLAUDIA
- IRIS

+140,000 Conscientious employees

AENOR GESTIÓN DE LA CALIDAD ER-0343/2008
AENOR SEGURIDAD INFORMACIÓN SI-0002/2006
AENOR GESTIÓN SERVICIOS TI STI-0001/2011
AENOR GESTIÓN I+D+i ID-0066/2010
AENOR GESTIÓN CONTINUIDAD NEGOCIO SCN-2022/0006
AENOR GESTIÓN AMBIENTAL GA-2013/0358
ens
IQNET RECOGNIZED CERTIFICATION

CCN CERTIFICATE
CCN CERTIFICATE
AUTHORIZED TO USE CERT
CERTIFIED BY TI TRUSTED INTRODUCER
FIRST MEMBER

Red Nacional de SOC
GoI Member

gloria
carmen Advanced cyberintelligence

INDEX

R2D2

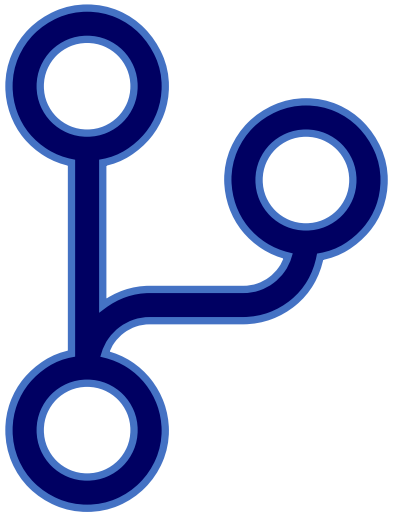
- Project
- Products
- Goals

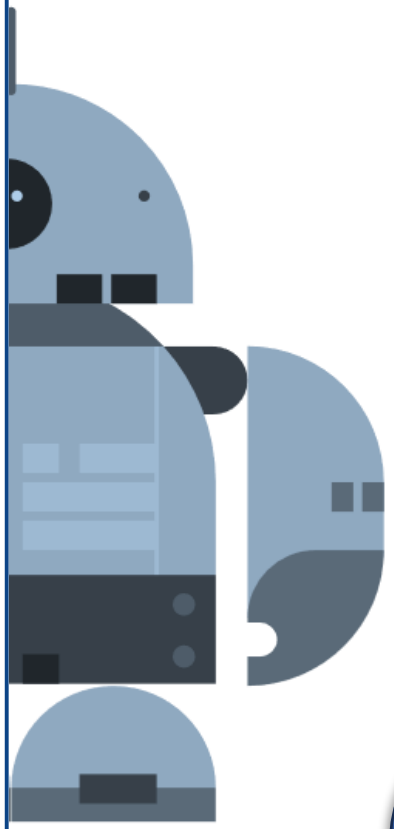
PRECOG

- APTs
- CARMEN
- S2TH
- Dynamic Risk

C3PO

- Assessment
- Risk Evaluation
- Knowledge Sharing





Reliability, **R**esilience and **D**efence technologies for the gri**d**

Time Lapse:

Start: Oct.'22 – End:Sept.'25

Duration: 36 months

Web Page: https://r2d2project.eu/

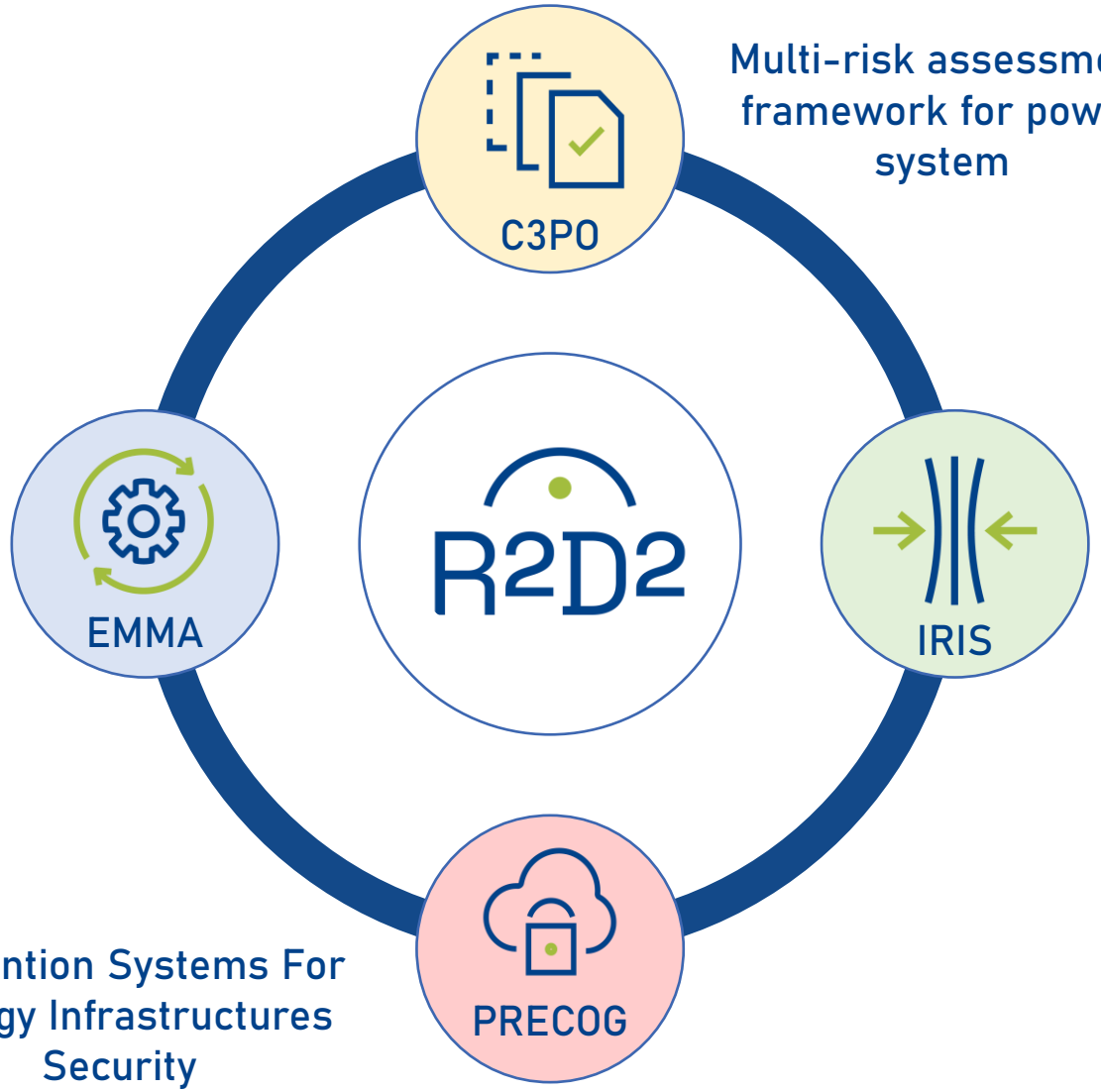
4 Pilot Locations

4 Products

17 European Partners

PRODUCTS

R2D2



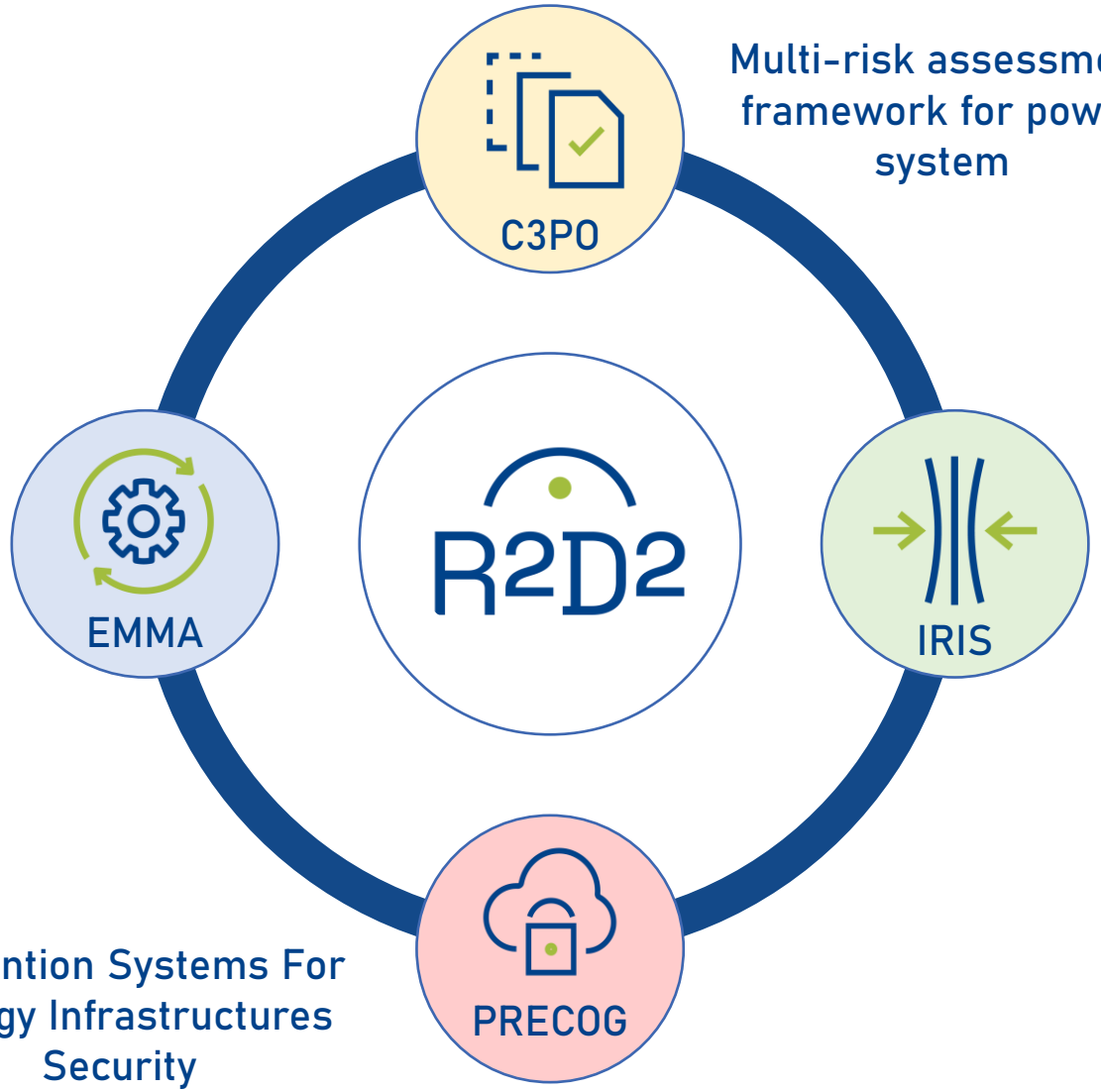
Before Event
- P1 - C3PO
- P3 - PRECOG
- P4 - EMMA

During Event
- P2 - IRIS
- P3 - PRECOG

After Event
- P3 - PRECOG
- P4 - EMMA

PRODUCTS

R2D2



Before Event
- P1-C3PO
- P3 - PRECOG
- P4 - EMMA

During Event
- P2 - IRIS
- P3 - PRECOG

After Event
- P3- PRECOG
- P4 - EMMA

GOALS

1. To contribute to the improvement of the overall security and resiliency in power system

- 4 products to cover several aspects
- Holistic and multidisciplinary Approach

2. To increase the cyber-security and cyber-resilience in OT and IT of the EPES

- Monitoring, detecting and misleading attacks
- Development new tools for attack detection
- Dynamic cyber-risk assessment and management

3. Contribute to the development of a shared knowledge

- Sharing best practices, methodologies, etc…
- Communication and dissemination activities
- Cooperation with Bridge and other H.EU projects

PRECOG

APTs – Advanced Persistent Threats

- **APT**: describes an attack campaign in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network to mine highly sensitive data.

- **Threat Hunting**: proactive and reiterative review of the organization's communications through the monitoring of APT group techniques.

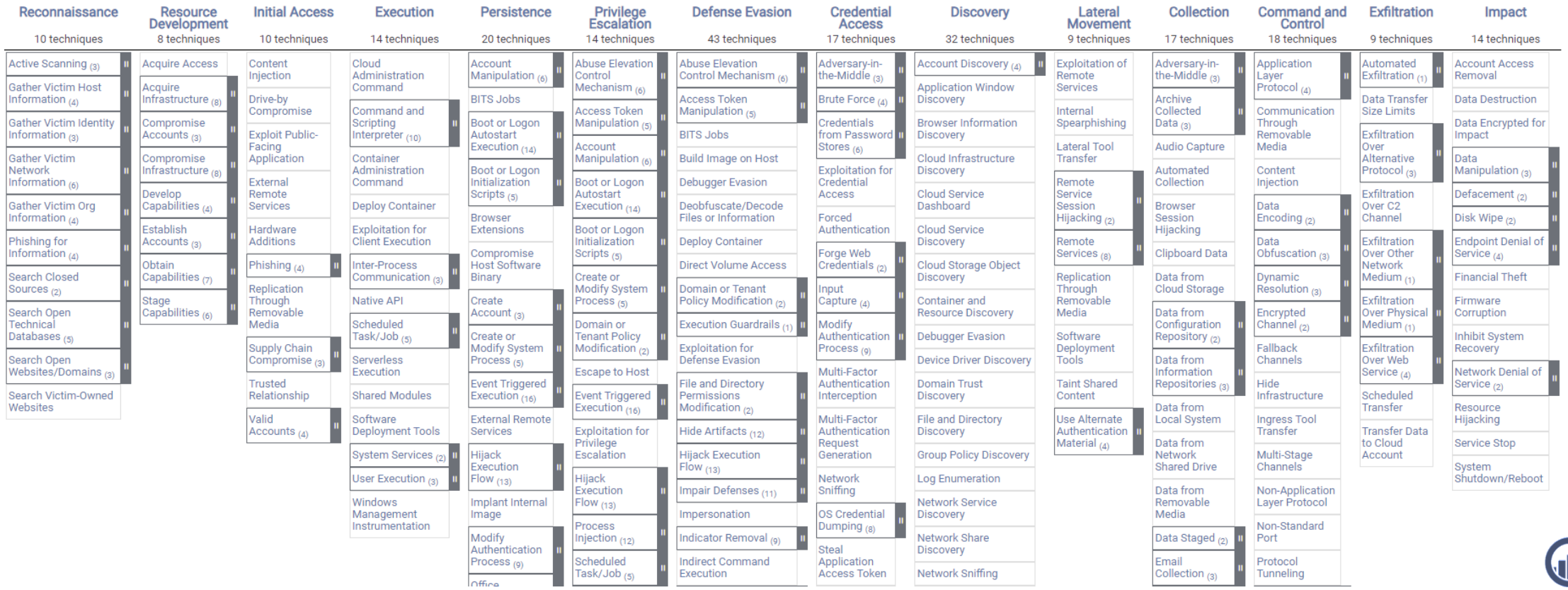
APTs – LifeCycle & Traditional Detection

Detecting APTs presents multiple challenges due to the sophistication and adaptability of these attacks:

- Evasion Techniques: very specific malware, encryption and obfuscation techniques …
- Limitations of Traditional Detection Techniques: late reactions, nosise in form of false positives…
- Need for Dynamic Approach based on new and advanced technologies such as AI.

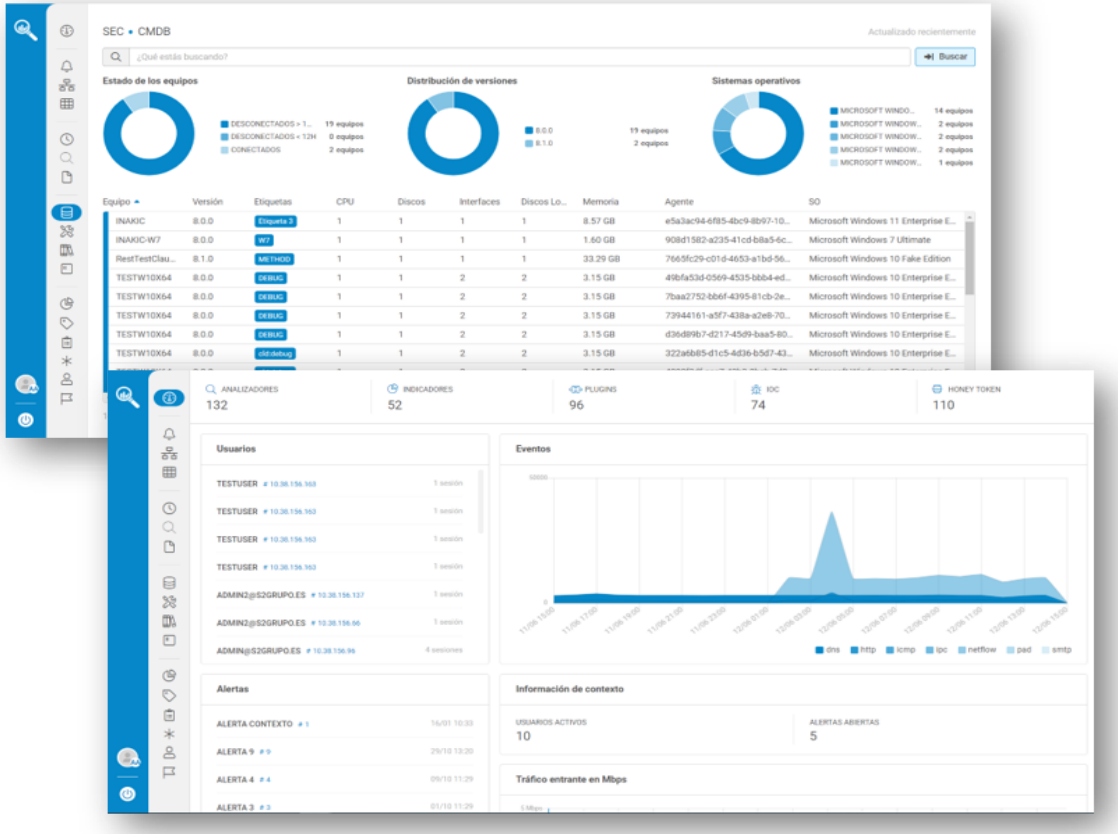
APTs – MITRE ATT&CK MATRIX

Public Database on actors' tactics, techniques, and procedures based on observed behaviour.

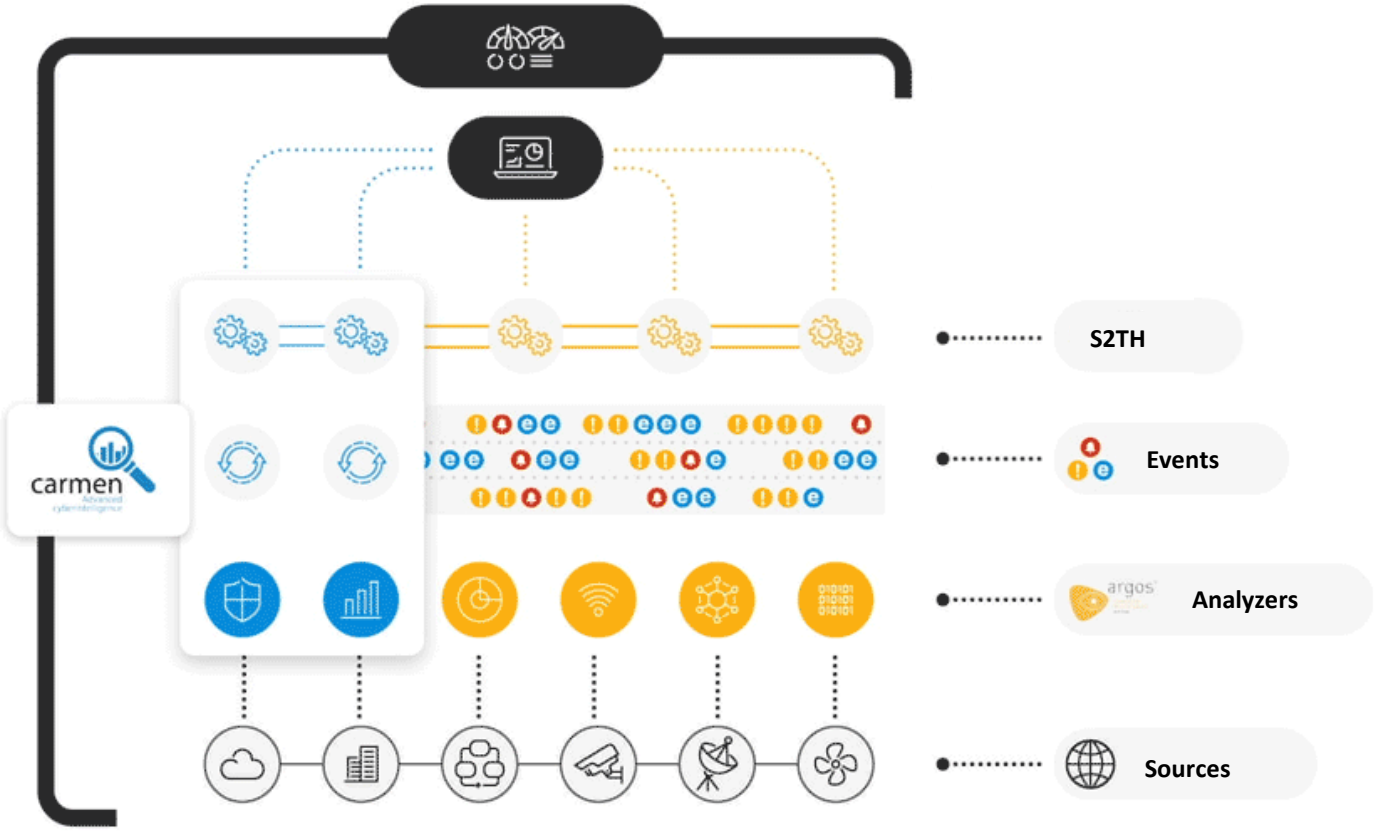


APTs – CARMEN Tool

- CARMEN is S2 Grupo's APT compromise detection tool.
- CARMEN protects organizations by acquiring, processing and analyzing their traffic, to detect anomalies and misuse.
- It allows to protect systems in the intrusion phase (Breach Detecting) by detecting infection mechanisms, and to find threats in the persistence phase thanks to the identification of external and lateral movements.

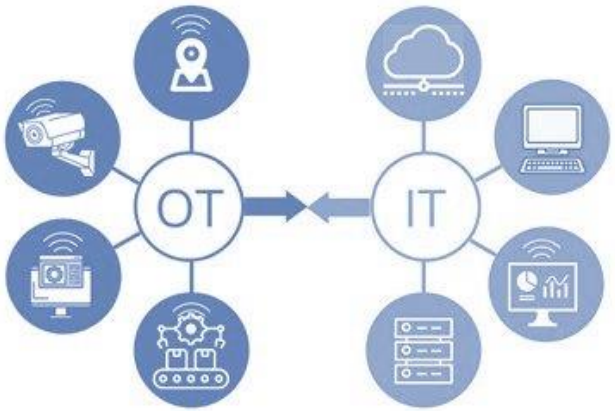


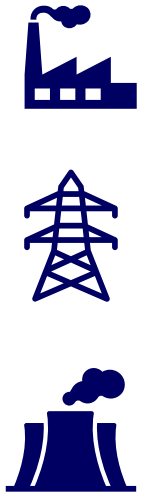
APTs – CARMEN Workflow



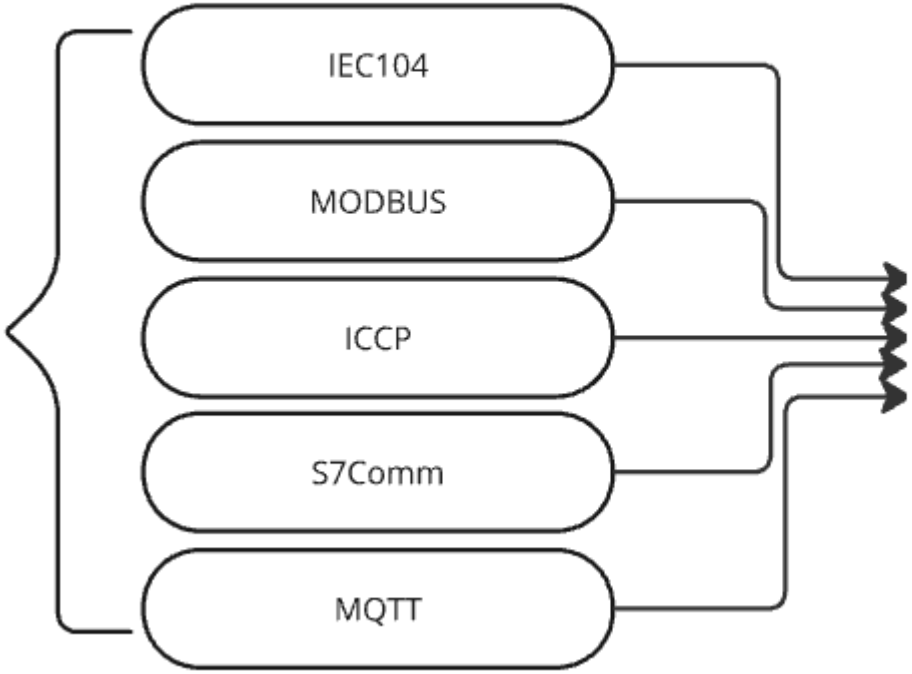
APTs - Dissectors & Analyzers

INPUT DATA





OT DISSECTORS



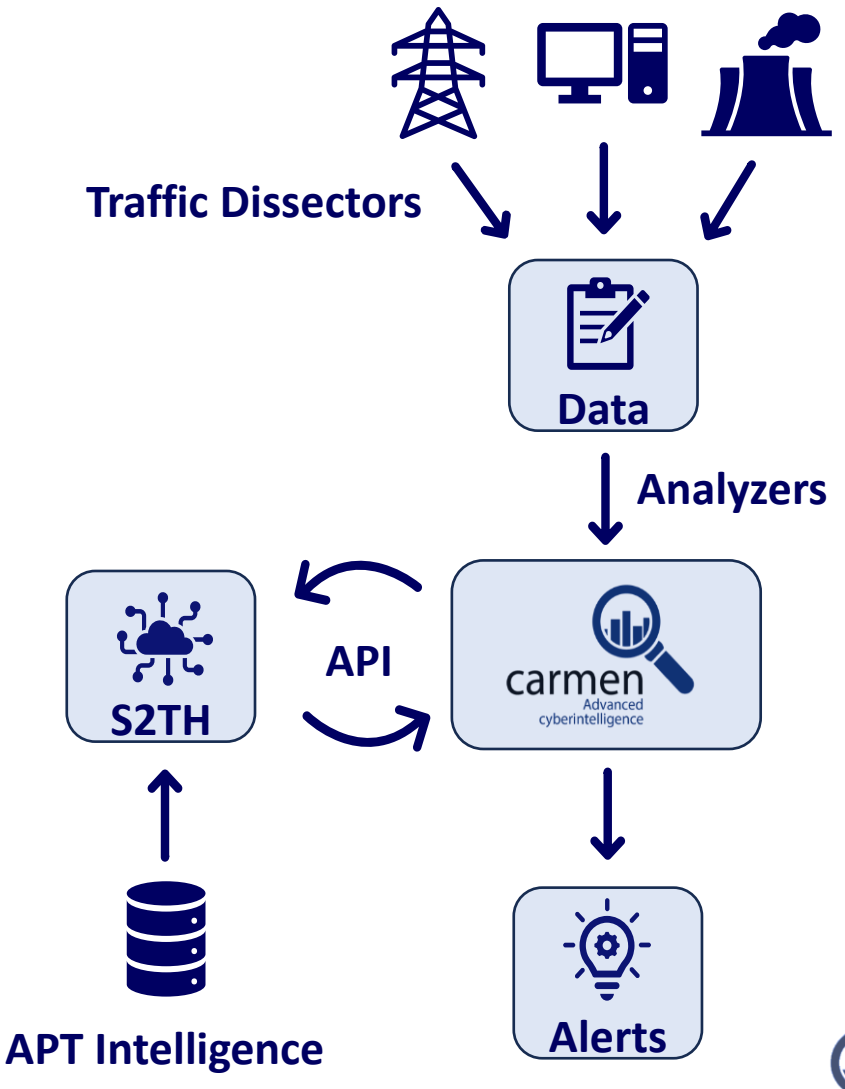
DATA
ANALYZERS

S2TH – Tool Architecture

External Module that combines:

- **Threat Intelligence**: provides the baseline intelligence against which to compare.
- **Artificial Intelligence**: helps to find similarities between input traffic and baseline intelligence.

Output alerts are connected to a correlator engine that estimates the final risk of APT.



Normalization – Generative AI

Data in multiple formats, from the intelligence base to the results of CARMEN's analysers.

Gen-AI is proposed as a normalizer.

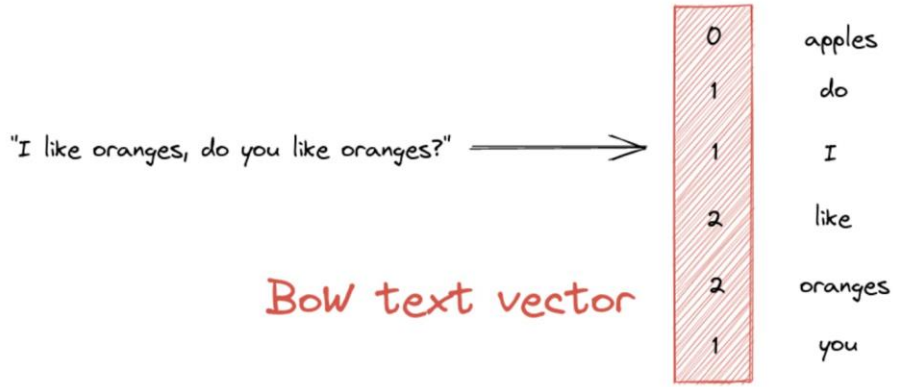
- List of standardisation rules needed: tags, parameters, negation operators…
- AI Agent with access to MITRE ATT&CK Framework.
- Reference examples for learning.

NLP (Text to Numeric Vectors)

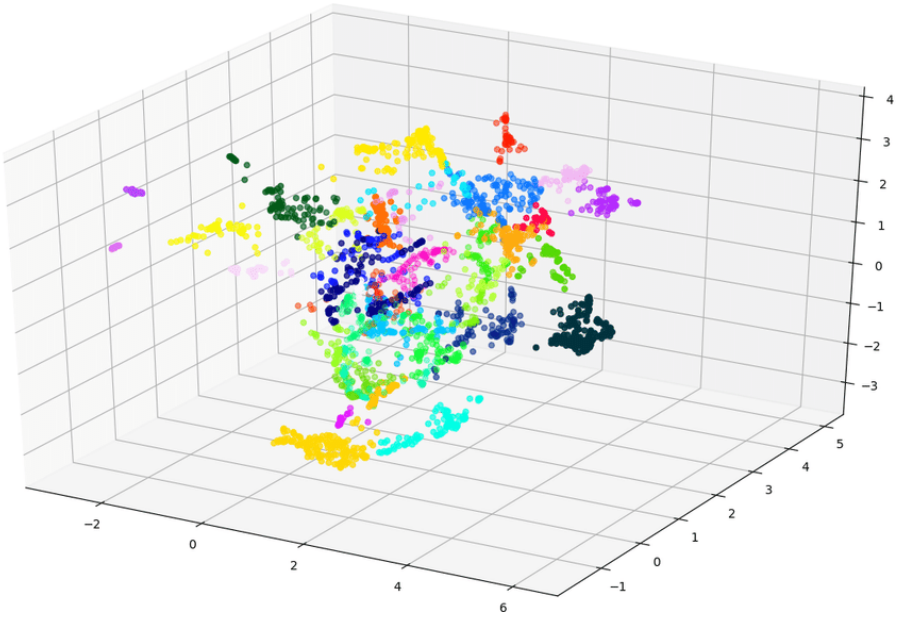
APT Baseline Intelligence

APT	Analyzer
OPERA1ER	[T1102] Execution with protocol -HTTP- with SLD -ddns.net-
APT41	[T1129] Execution with CommandLine -.docx.exe-
Worok	[T1040] Execution with CommandLine -Tq w M-
Sandworm Team	[T0867] Load dll with ImageLoad -cscript C:\Backinfo\ufn.vbs
Temp. Veles	[T0853] Execution with CommandLine -py2exe Win executable -- trilog.exe

Text Embedding



N-Dimensional Projections

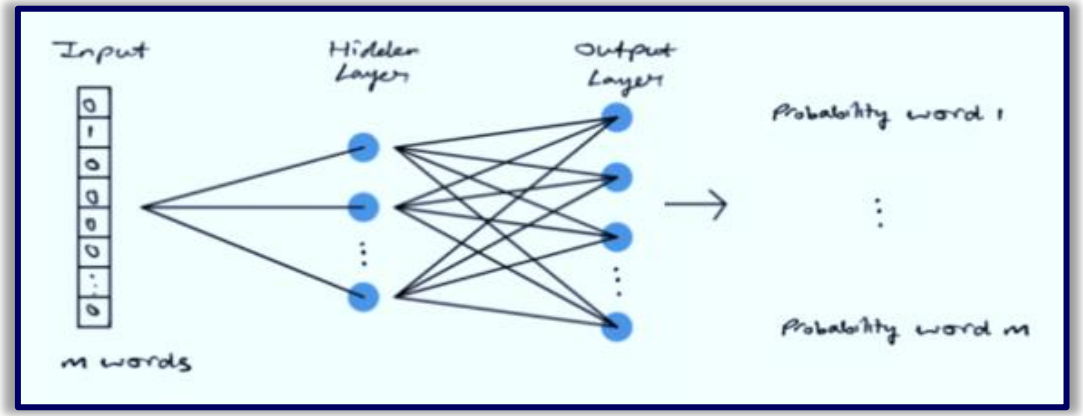


NLP – Word2Vec

It is based on the idea that the meaning of a word can be inferred from neighbouring words.

It uses a neural network model where, given a vocabulary of size M, the inputs are one-hot vectors.

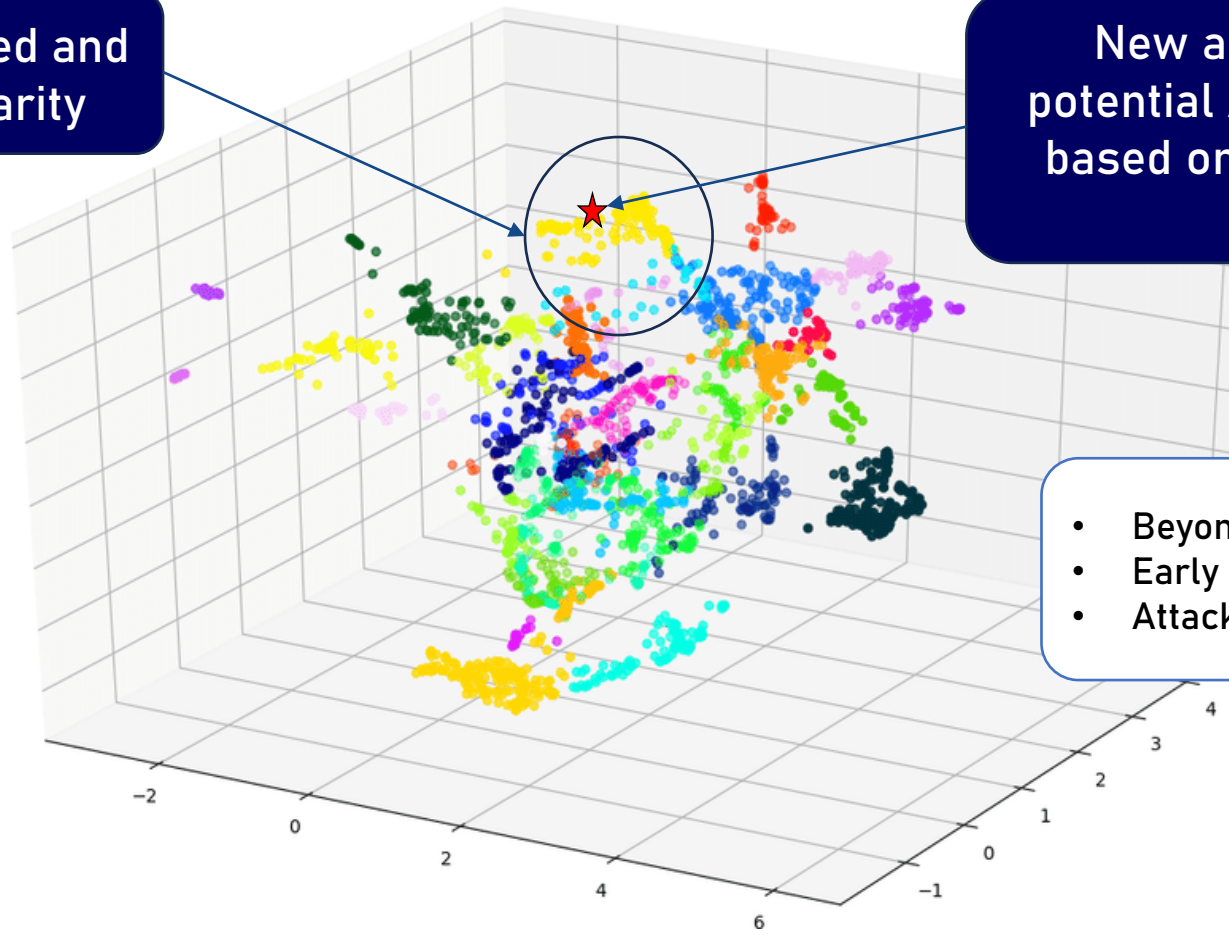
- Inputs are one-hot vectors, matrices (1 x M) with a single non-zero entry that identifies the vocabulary word it represents.
- The outputs represent the probabilistic similarity of the input to each word in the corpus.



N-Dimensional Projections

Known TTPs mapped and grouped by similarity

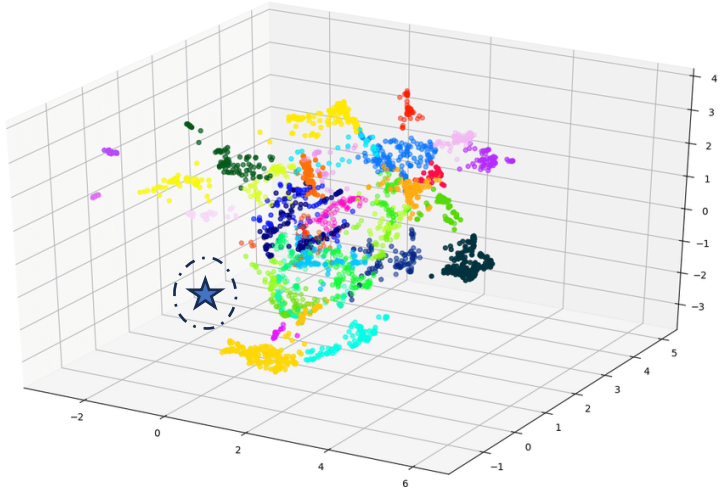
New activity is mapped and potential APT activity is assessed based on its similarity to known APTs activities



- Beyond static signature patterns
- Early detection
- Attack attribution by similarity

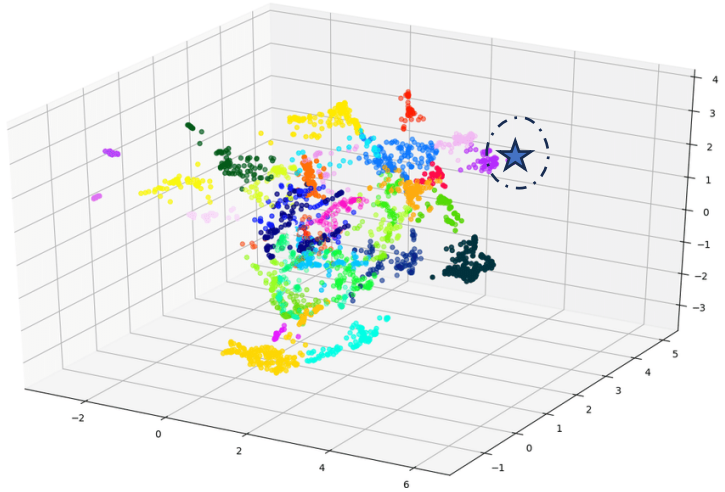
APT Similarities

Execution with Commandline - rundll32.exe C:\Windows\system32\davclnt.dll with parentcommandline C:\Windows\system32\svchost.exe -k LocalService -p -s WebClient



Normalized Traffic

Execution with Commandline - "c:\windows\system32\powershell.exe" -noprofile -executionpolicy bypass "(get-netfirewallsetting -policystore activestore).activeprofile"

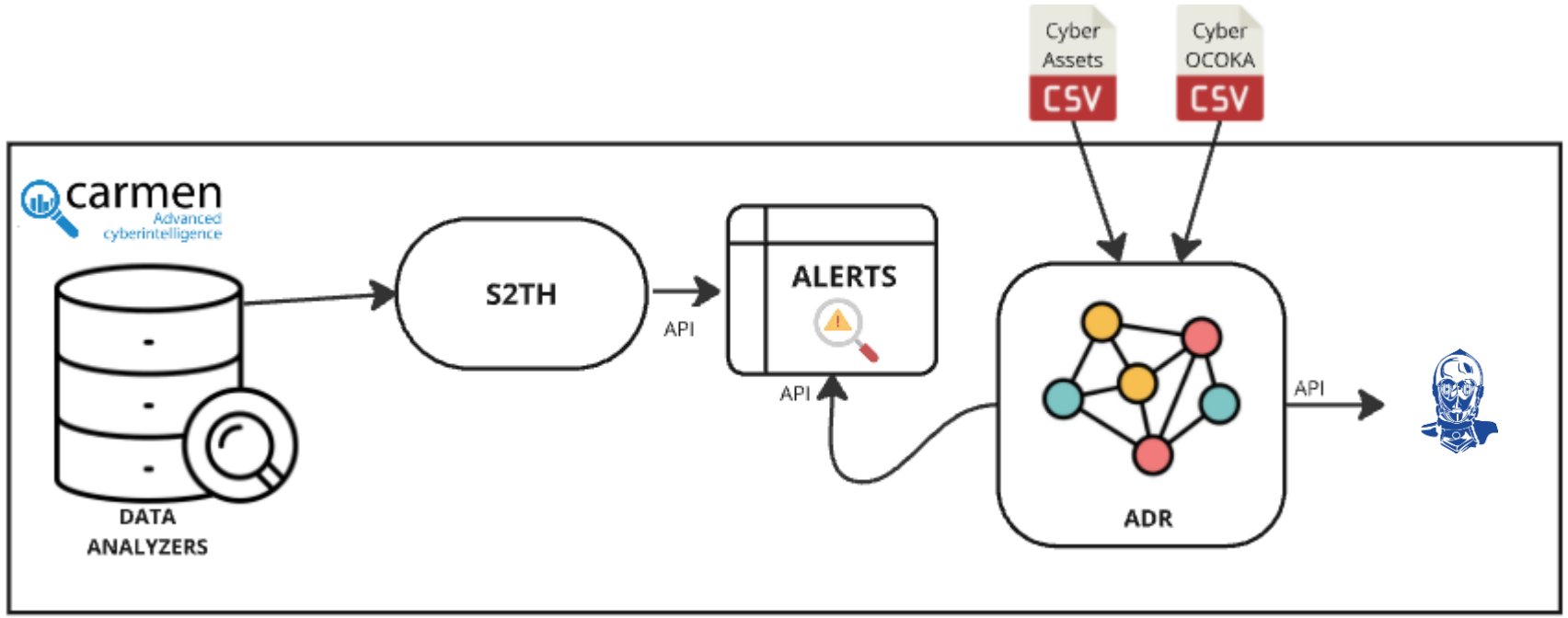


Alerts Detected

APT	BackdoorDiplomacy
Analyzer	Ejecución con CommandLine powershell -ExecutionPolicy Bypass

ADR (Dynamic Risk Analysis)

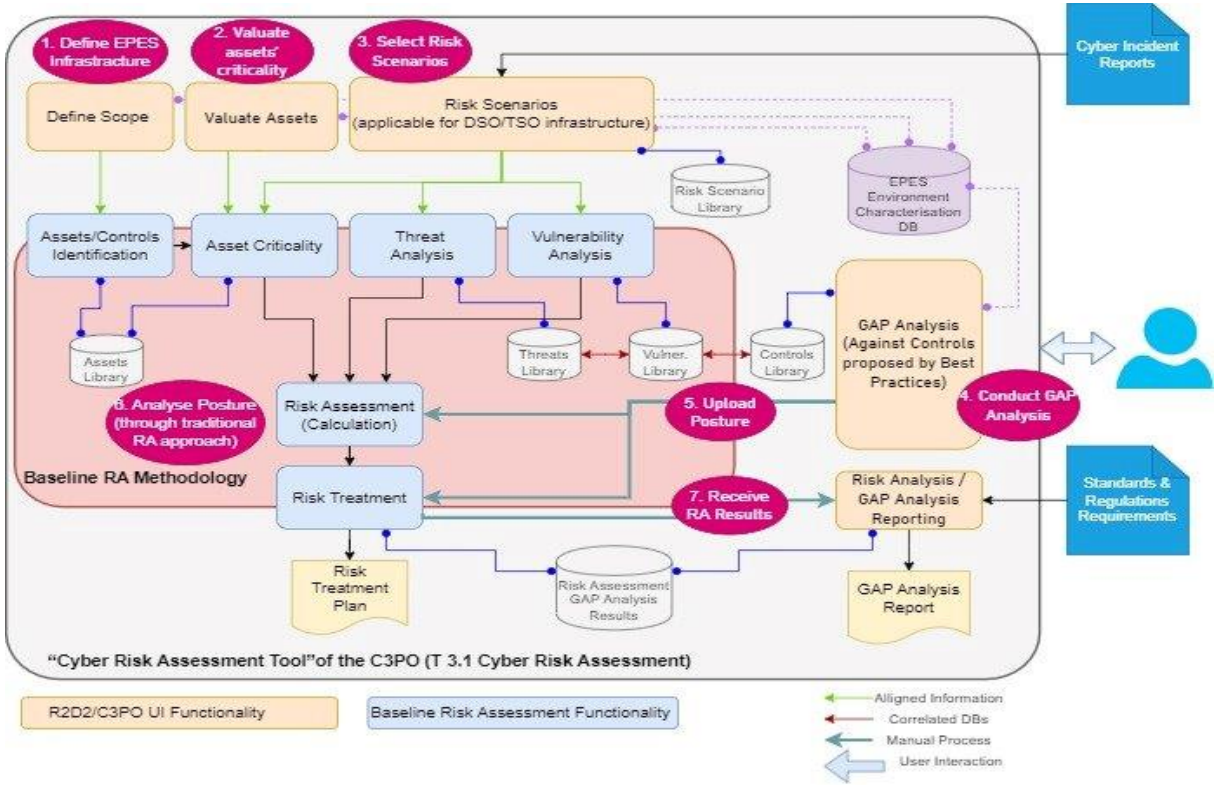
ADR Calculates the probability that an APT group will use a particular technique on an asset considering all possible routes between an initial access asset and a key terrain.



C3PO

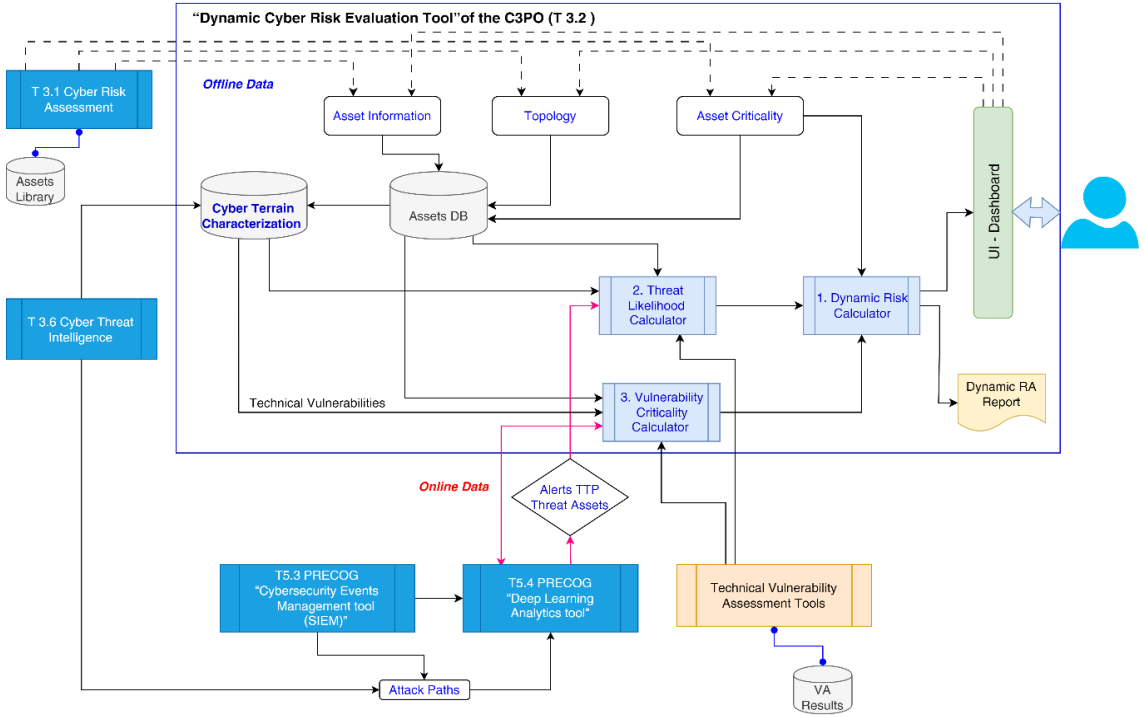
Cyber Risk Assessment

1. Assets modeling and criticality specification
2. Cyber security risk assessment, considering cyber threats, vulnerabilities and attack scenarios.
3. Controls maturity specification / gap analysis
4. Standards specification (eg ISO27001, NIST, NIS2)
5. Mapping ISO | NIS2 | NIST 800-53"
6. MONARC compatibility (method and libraries)
7. Risk scenarios definition
8. Reporting Specification



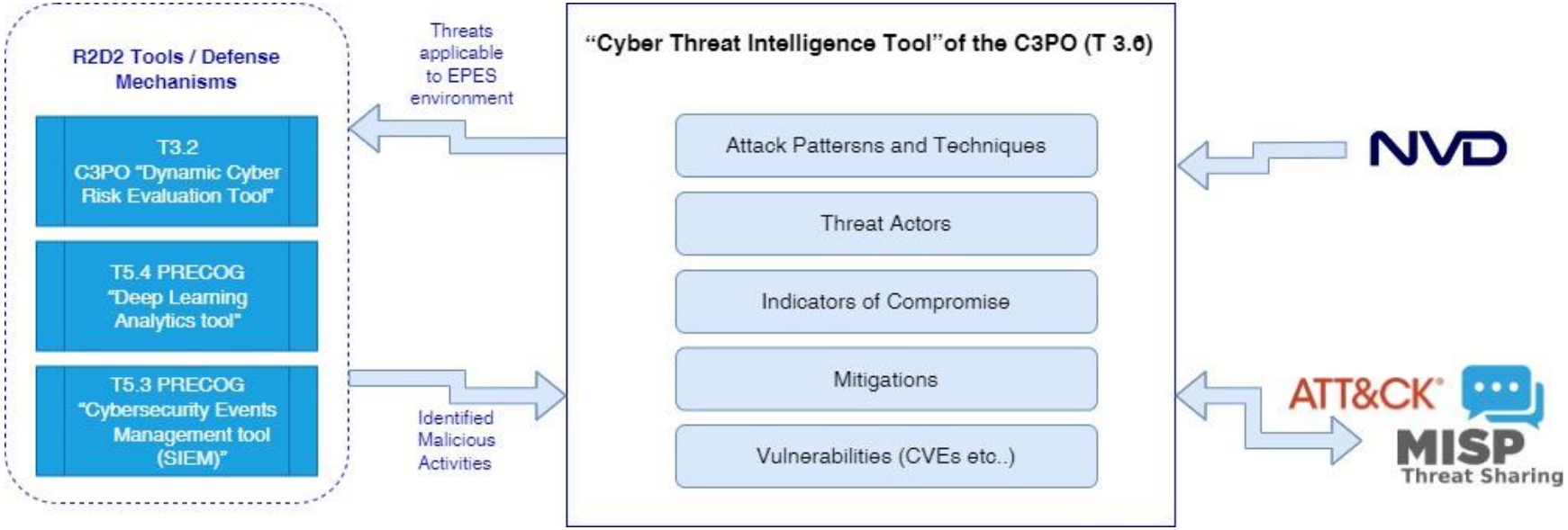
Dynamic Cyber Risk Status Evaluation

1. Collect target's environment information – automated and manual
2. Dynamically assess threats likelihood mapped to known attack patterns
3. Dynamically evaluate vulnerabilities severity considering controls/topology
4. Integrate cyber threat information provided by T3.6 CTI Tool
5. Dynamically assess risk levels
6. Fuzzy Cognitive Maps vulnerability severity assessment
7. EPSS exploitation probability
8. Identify likelihood of facing APT groups malicious activity
9. Connect to Deep Learning tool from T5.6
10. Provide risk reports



Knowledge sharing – Cyber Threat Intelligence

1. Deploy CTI platform (MISP)
2. Identify required sources and types of CTI
3. Develop interfaces (internal and external)
4. Prepare cyber threat information for dissemination



R2D2

THANK YOU!

/ Connect with us:

www.r2d2project.eu

@R2D2EU @R2D2project @R2D2EU