



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



Over **20 years** of cyber security experience



More than **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





R2D2



- Project
- Products
- Goals

PRECOG

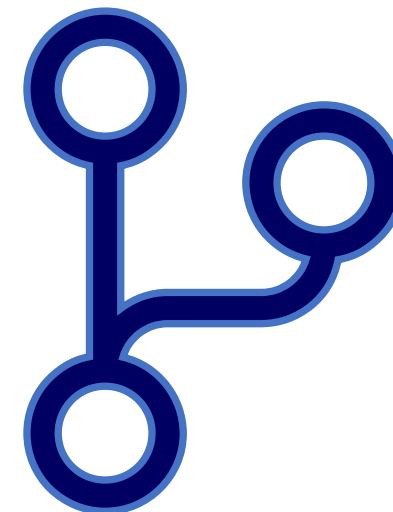


- APTs
- CARMEN
- S2TH
- Dynamic Risk

C3PO



- Assessment
- Risk Evaluation
- Knowledge Sharing





Reliability, Resilience and Defence technologies for the grid

Time Lapse:

Start: Oct.'22 – End:Sept.'25

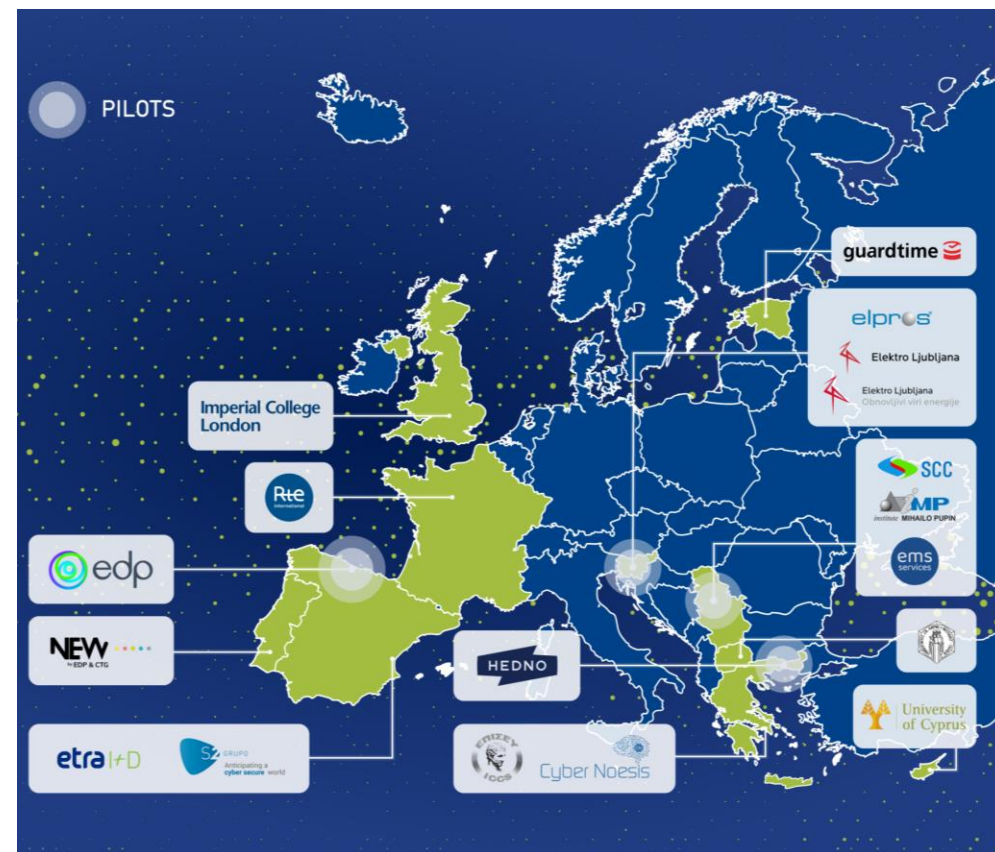
Duration: 36 months

Web Page: <https://r2d2project.eu/>

4 Pilot Locations

4 Products

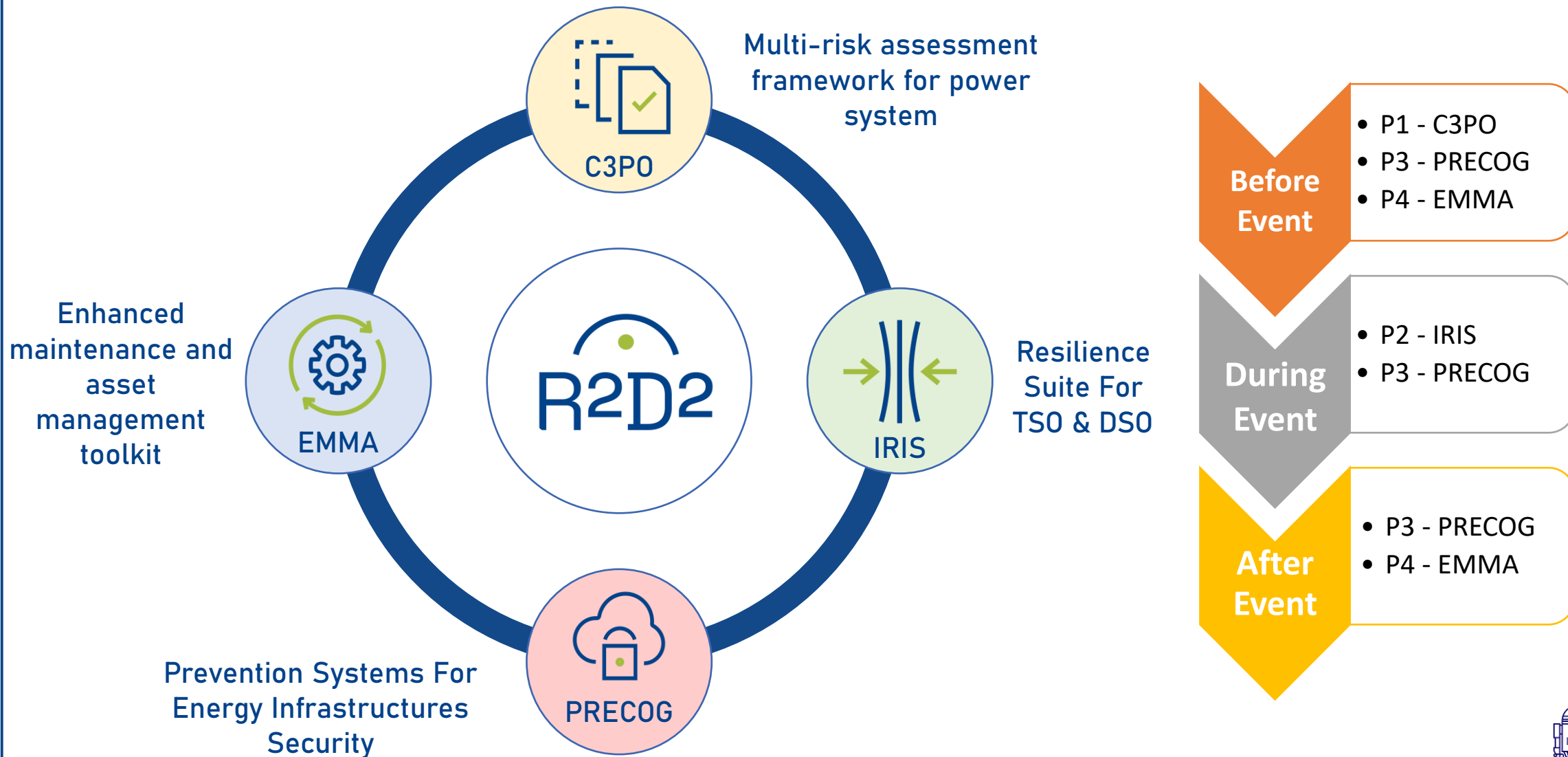
17 European Partners





PRODUCTS

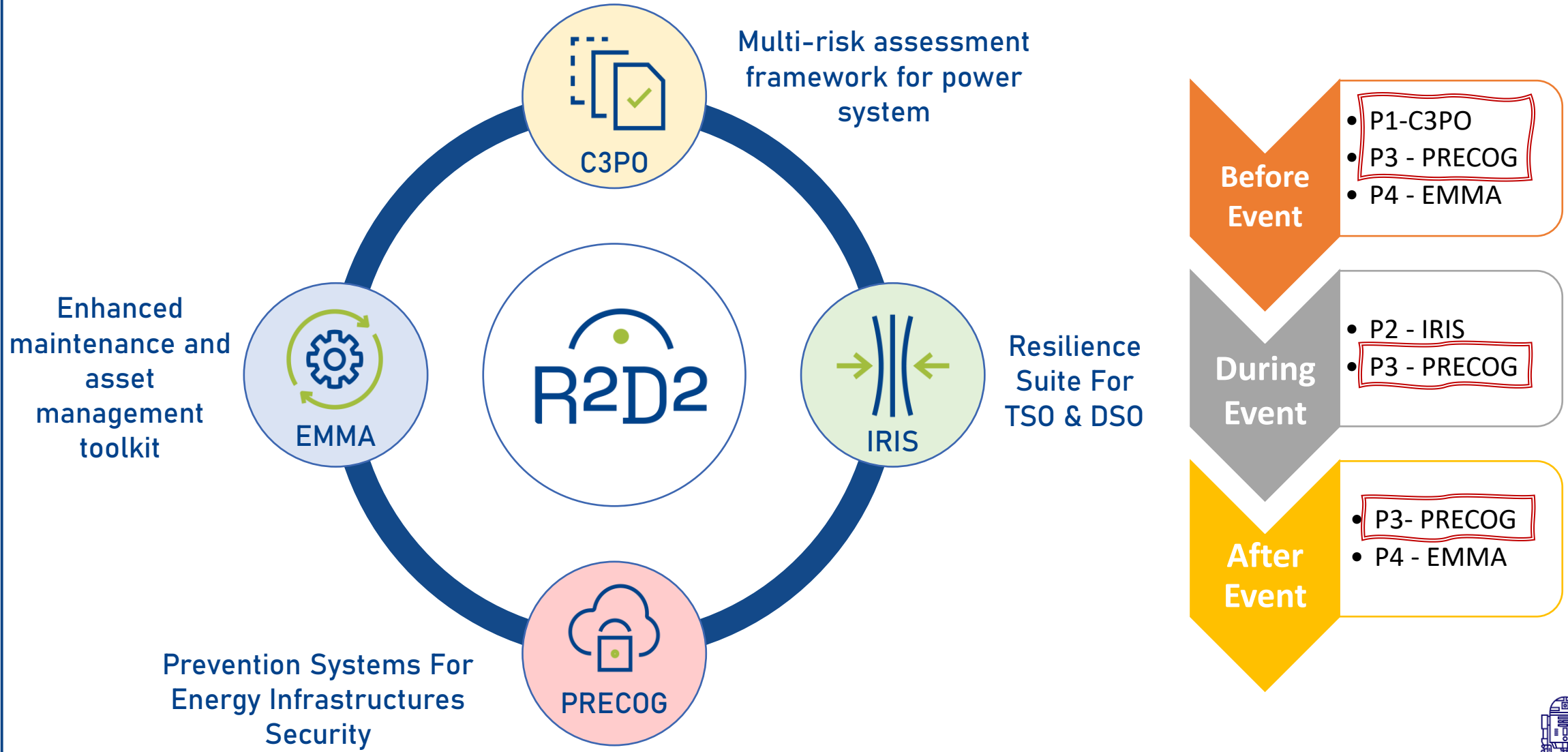
R2D2





PRODUCTS

R2D2





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 – 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, noise in form of false positives...
- Need for Dynamic Approach based on new and advanced technologies such as AI.





APTs - MITRE ATT&CK MATRIX

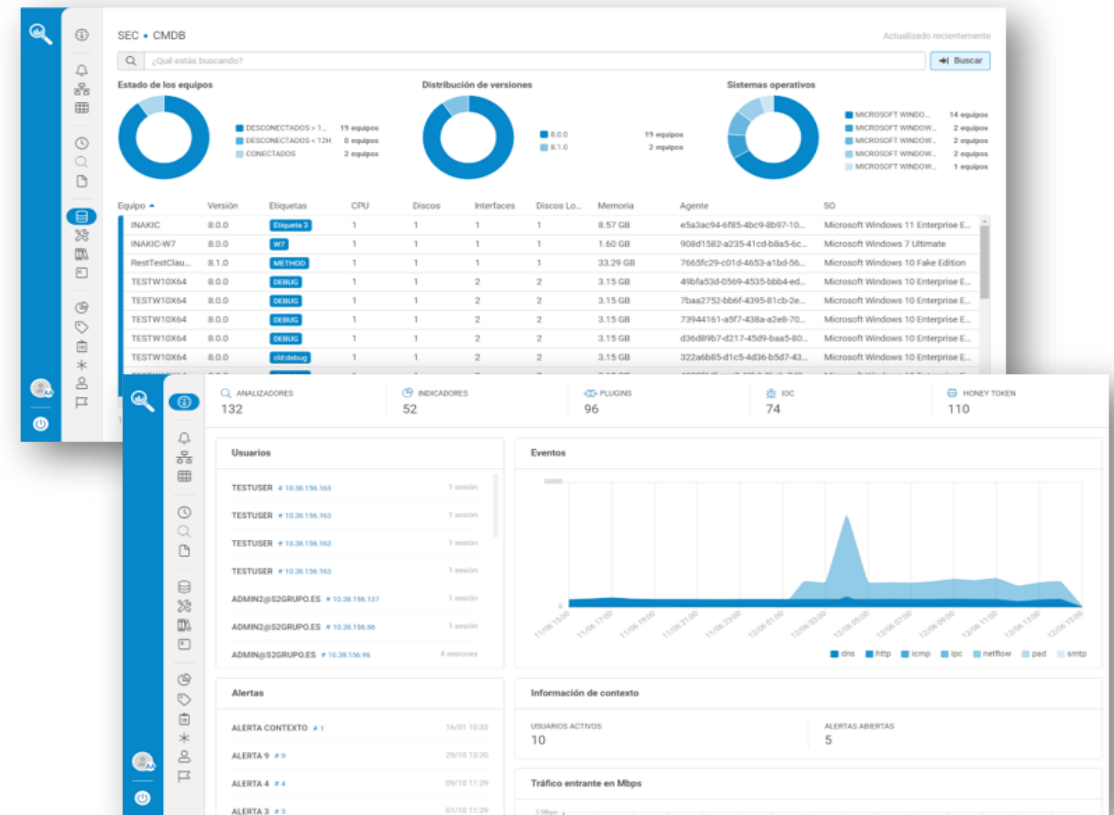
Public Database on actors' tactics, techniques, and procedures based on observed behaviour.

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (10)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Create or Modify System Process (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Domain or Tenant Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (5)	Domain or Tenant Policy Modification (2)	Direct Volume Access	Modify Authentication Process (9)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Exfiltration Over Web Service (2)	Financial Theft
Search Open Websites/Domains (3)	Trusted Relationship	Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Escape to Host	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Hide Infrastructure	Exfiltration Over Web Service (2)	Firmware Corruption
Search Victim-Owned Websites	Valid Accounts (4)	Valid Accounts (4)	Shared Modules	Event Triggered Execution (16)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Ingress Tool Transfer	Network Denial of Service (2)	Inhibit System Recovery
			Software Deployment Tools	External Remote Services	Hijack Execution Flow (13)	Hide Artifacts (12)	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels	Resource Hijacking	Service Stop
			System Services (2)	Hijack Execution Flow (13)	Hijack Execution Flow (13)	Hijack Execution Flow (13)	OS Credential Dumping (8)	File and Directory Discovery		Data from Removable Media	Non-Application Layer Protocol	System Shutdown/Reboot	System Shutdown/Reboot
			User Execution (3)	Implant Internal Image	Process Injection (12)	Impair Defenses (11)	Steal Application Access Token	Group Policy Discovery		Data Staged (2)	Non-Standard Port		
			Windows Management Instrumentation	Modify Authentication Process (9)	Scheduled Task/Job (5)	Impersonation		Log Enumeration		Email Collection (3)	Protocol Tunneling		
				Scheduled Task/Job (5)		Indicator Removal (9)		Network Service Discovery					
						Indirect Command Execution		Network Share Discovery					
								Network Sniffing					

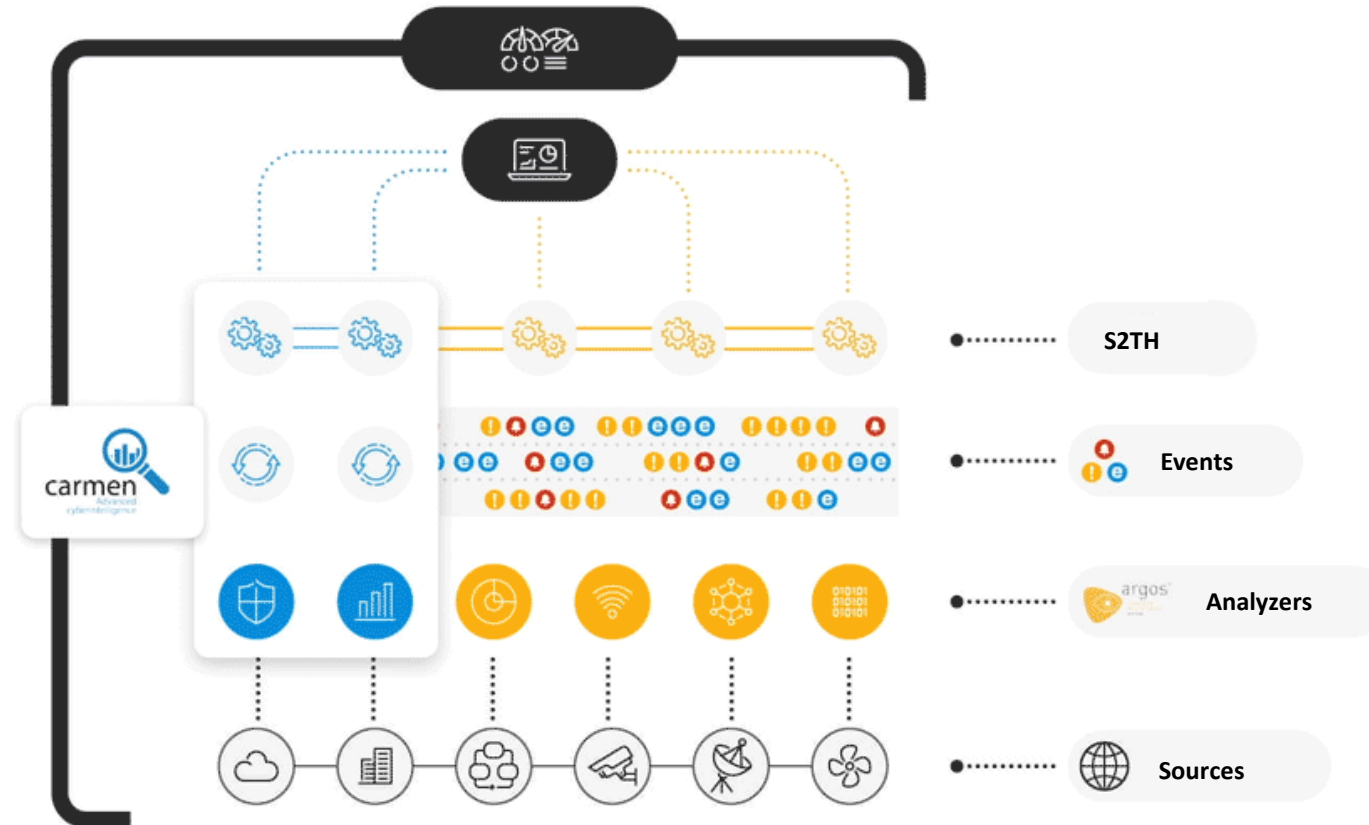


APTs – CARMEN Tool

- 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.

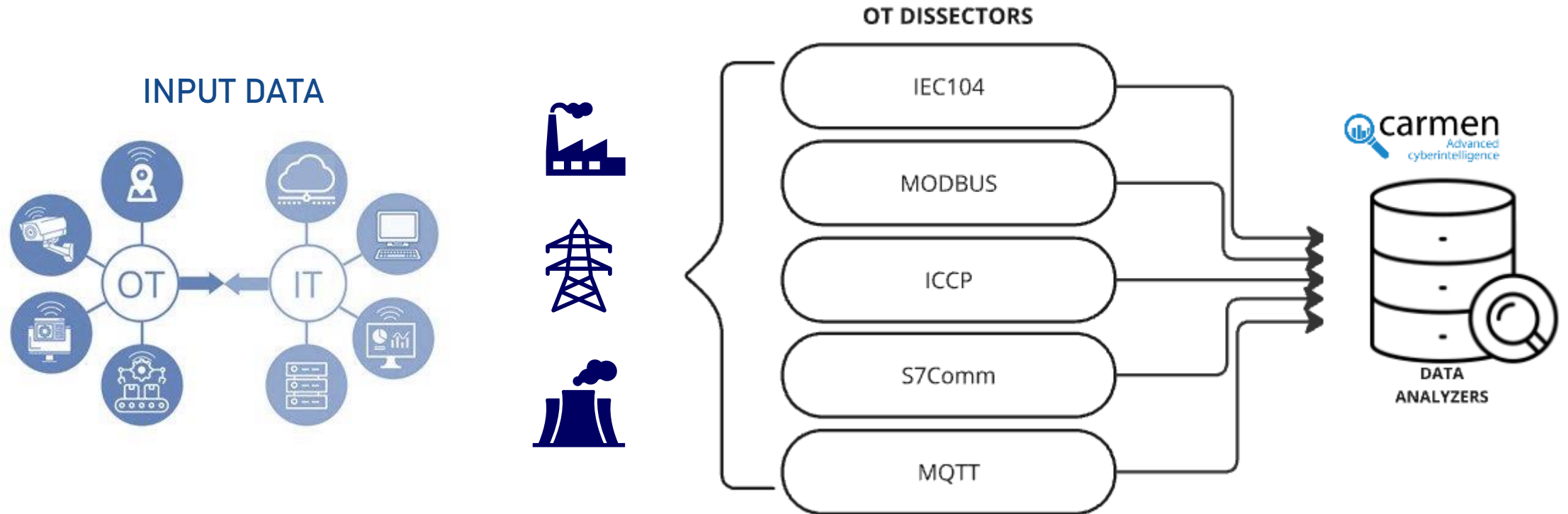


APTs – CARMEN Workflow





APTs - Dissectors & Analyzers



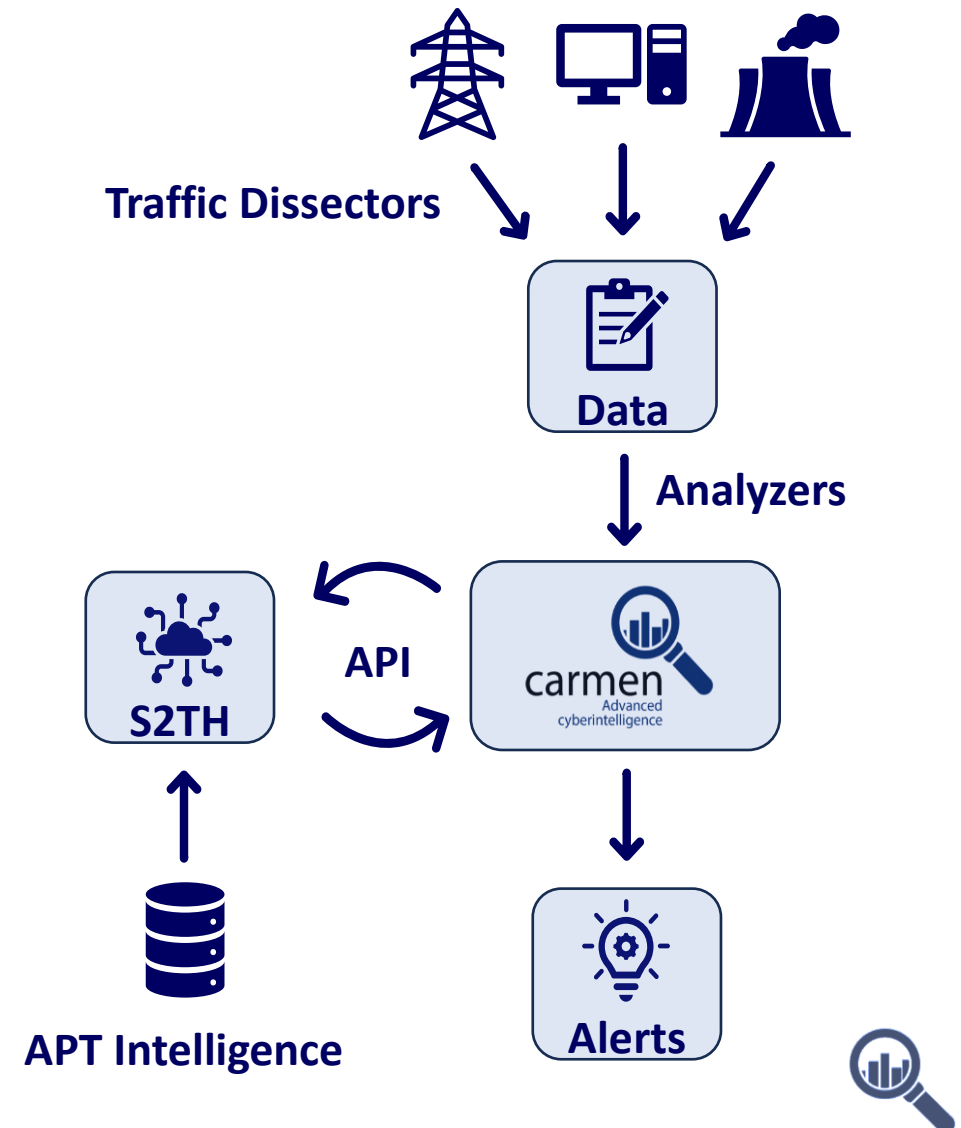


S2TH - Tool Architecture

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

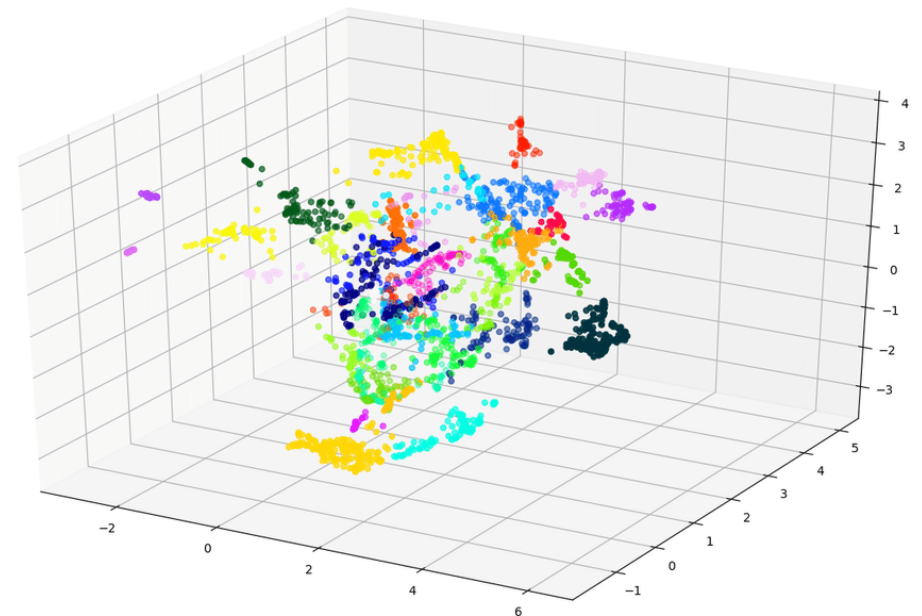
Text Embedding

"I like oranges, do you like oranges?"

0	apples
1	do
1	I
2	like
2	oranges
1	you

Bow text vector

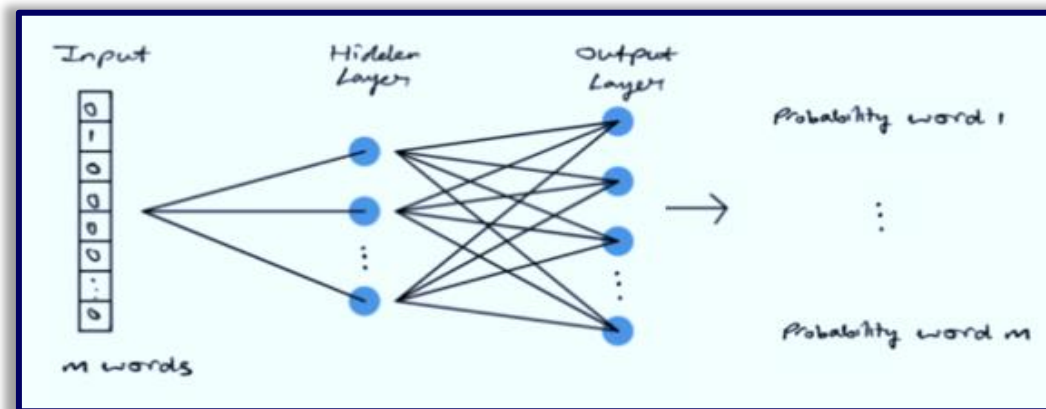
N-Dimensional Projections



NLP – Word2Vec

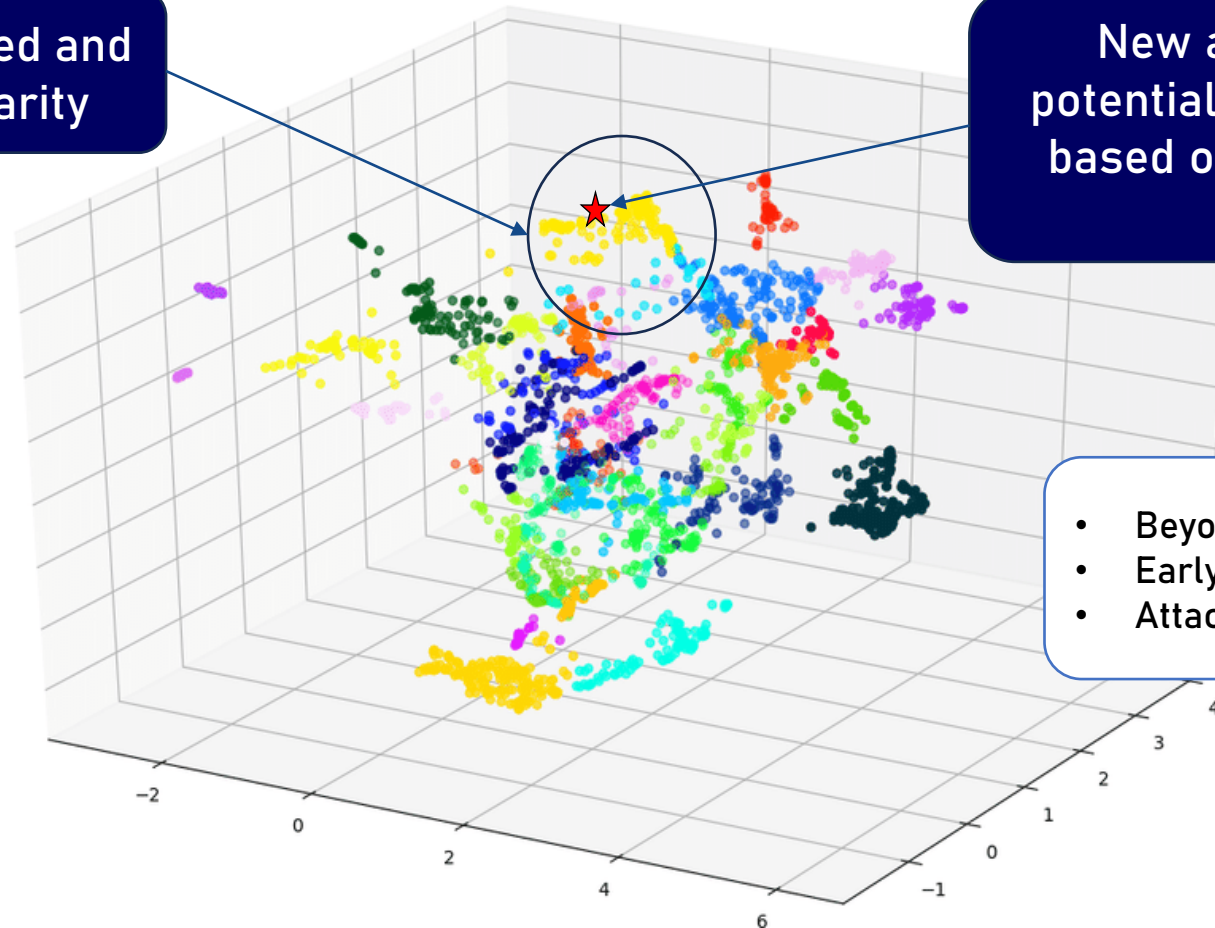
It is based on the idea that the meaning of a word can be inferred from neighbouring words. It uses a neural network model where, given a vocabulary of size M , the inputs are one-hot vectors.

- Inputs are one-hot vectors, matrices $(1 \times M)$ 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



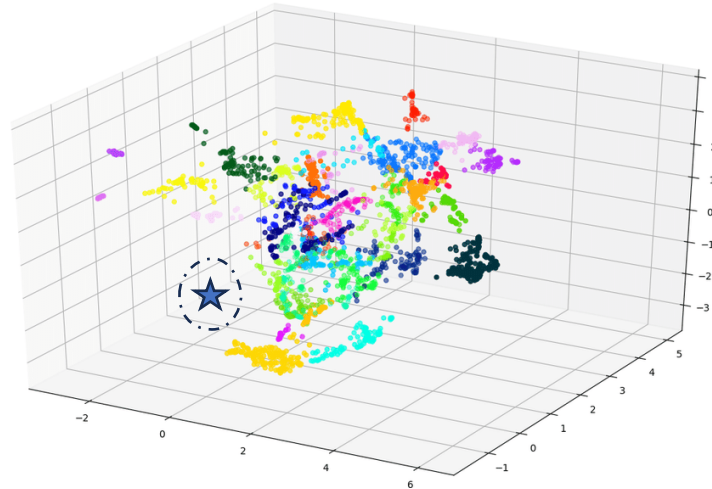
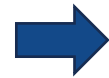
New activity is mapped and potential APT activity is assessed based on its similarity to known APTs activities

- 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

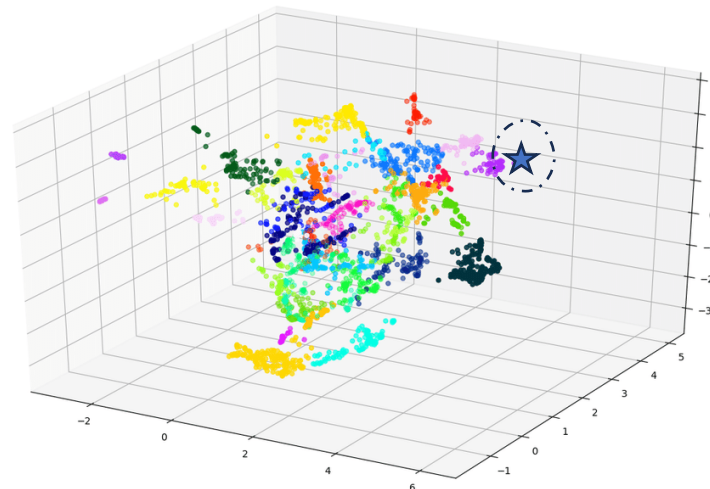


Alerts Detected



Normalized Traffic

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

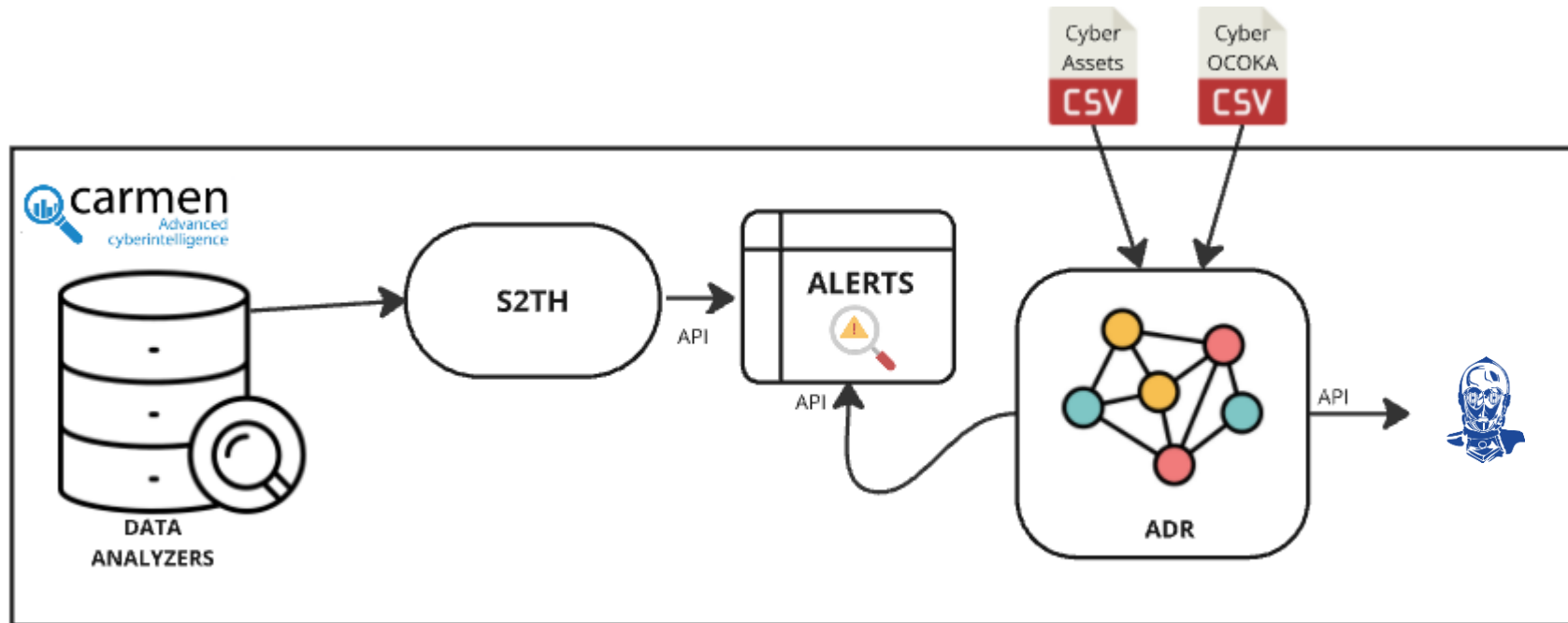


APT	BackdoorDiplomacy
Analyzer	Ejecución con CommandLine powershell - ExecutionPolicy Bypass



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.



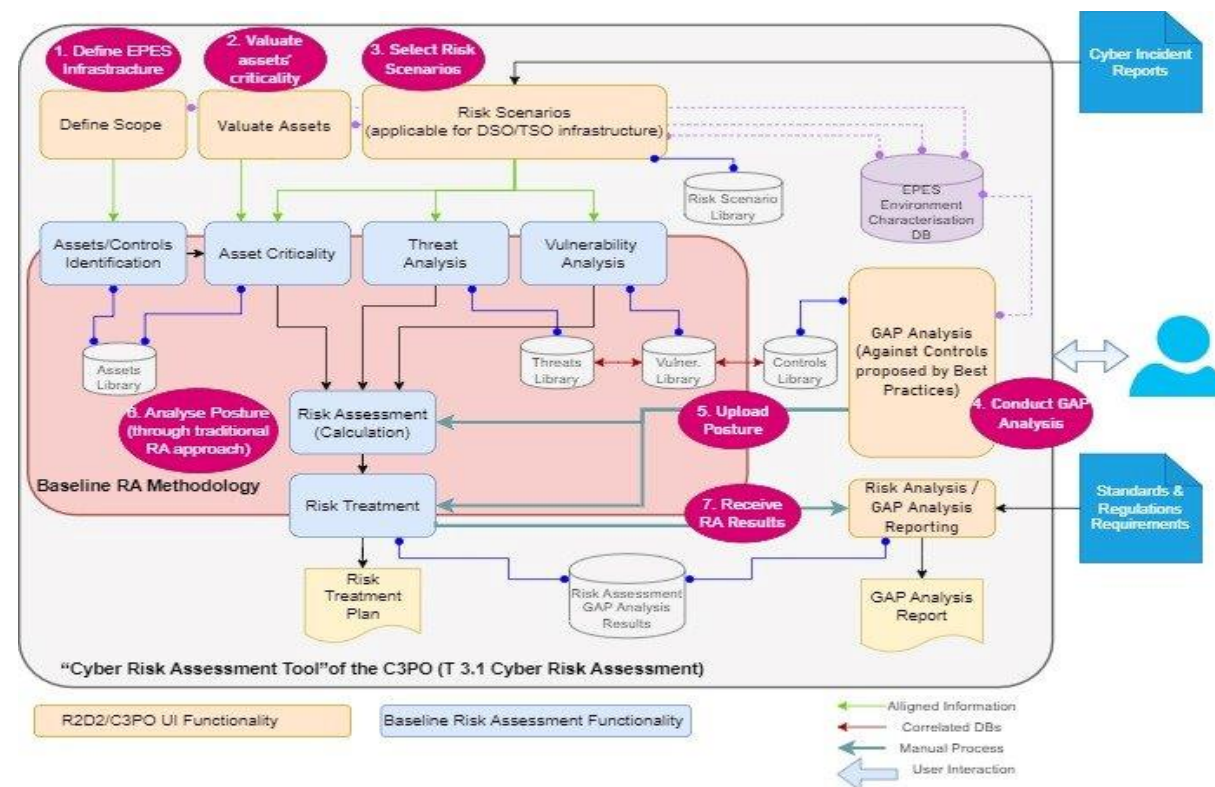


C3PO



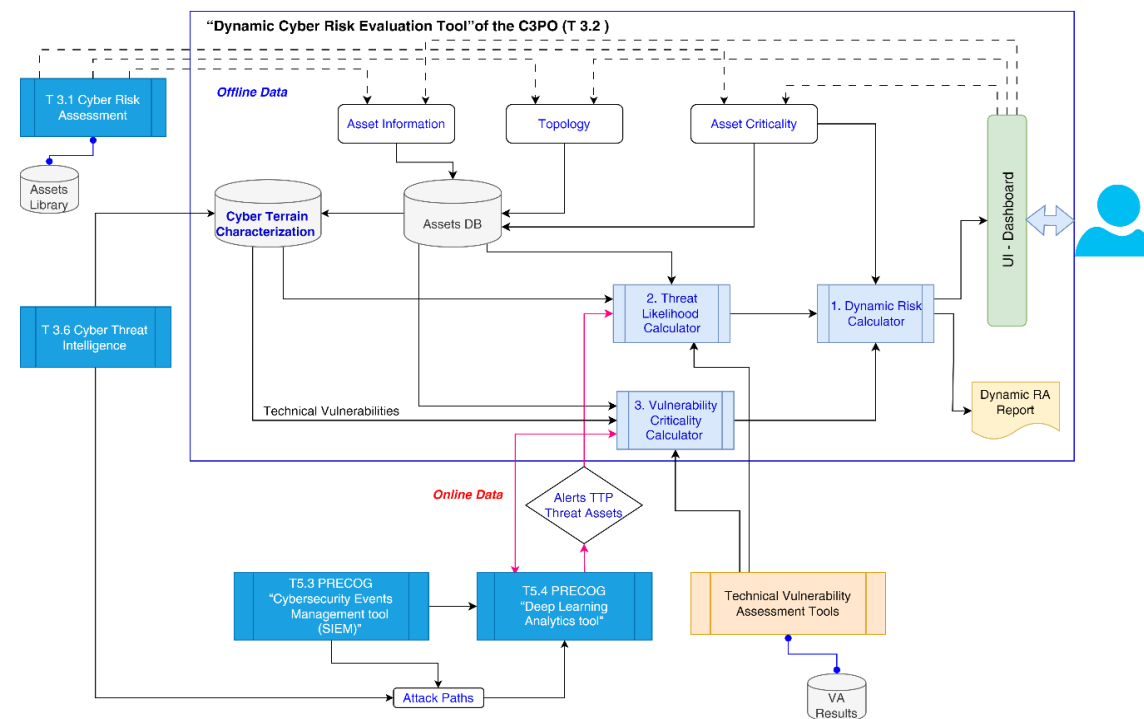
Cyber Risk Assessment

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



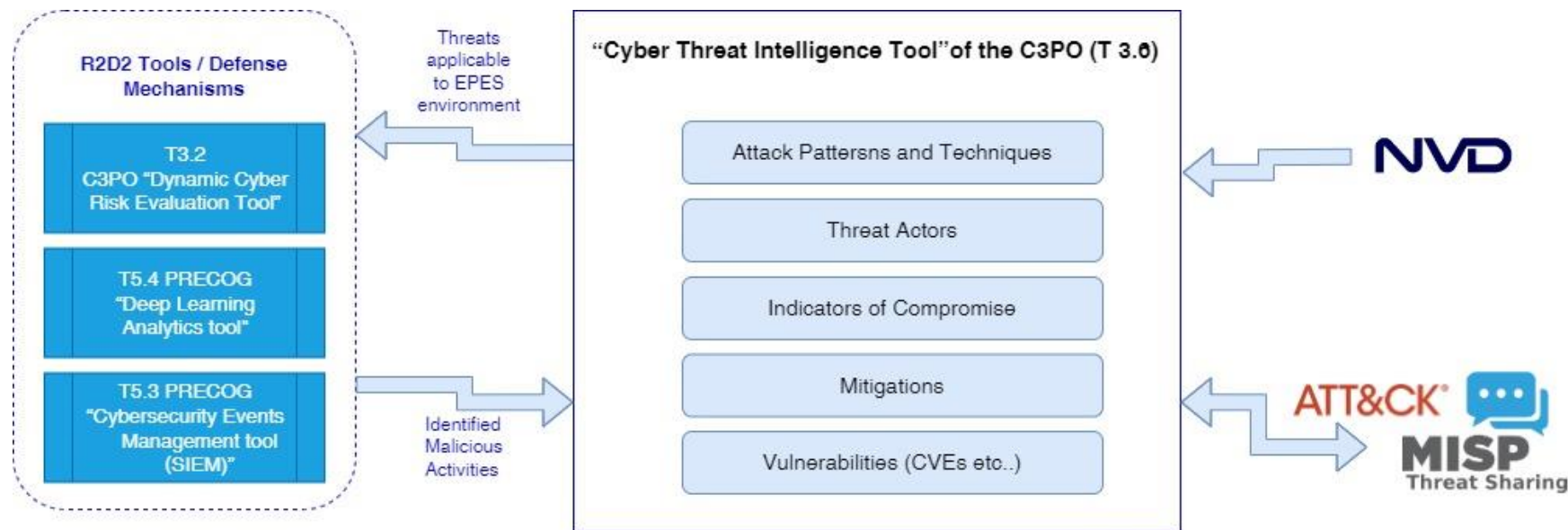
Dynamic Cyber Risk Status Evaluation

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





Elektro Ljubljana
Obnovljivi viri energije



Imperial College
London



R2D2

THANK YOU!

/ Connect with us:

www.r2d2project.eu

 @R2D2EU

 @R2D2project

 @R2D2EU