1 Resilience Orchestration, Automation & Response

ROAR: The 1st CACAO Editor & Orchestrator implemented worldwide; integrated in CACAO specification V2.0.

RPs: The most holistic playbook approach, and the 1st to use CACAO playbooks for Business Continuity.

2 Alerting, Reporting & Information Exchange

SMIR: Innovative tool that addresses lack of harmonization of mandatory incident reporting procedures – Facilitates the collection and reporting of incidents.

3 AI-assisted Situational Awareness, Prediction & Response

AutoML-based UEBA: Context-aware profiling of users and devices to detect and prevent malicious activity in real time.

SeBiS: Innovative training based on previous user behaviour.

CTI Discovery & Analytics: NLP-based tools to discover & extract CTI-relevant information from human readable sources.

TAC ontology: Aiming to be the industry standard for representing STIX 2.1 data using an ontology and populate knowledge graphs.

TII: Enhanced MISP synchronization tool to filter non-relevant information.

PMEM: Enhanced proactive real-time cyberattack prediction by dynamic model selection based on context.

CERCA: Dynamic risk assessment - in a qualitatively and quantitatively fashion.
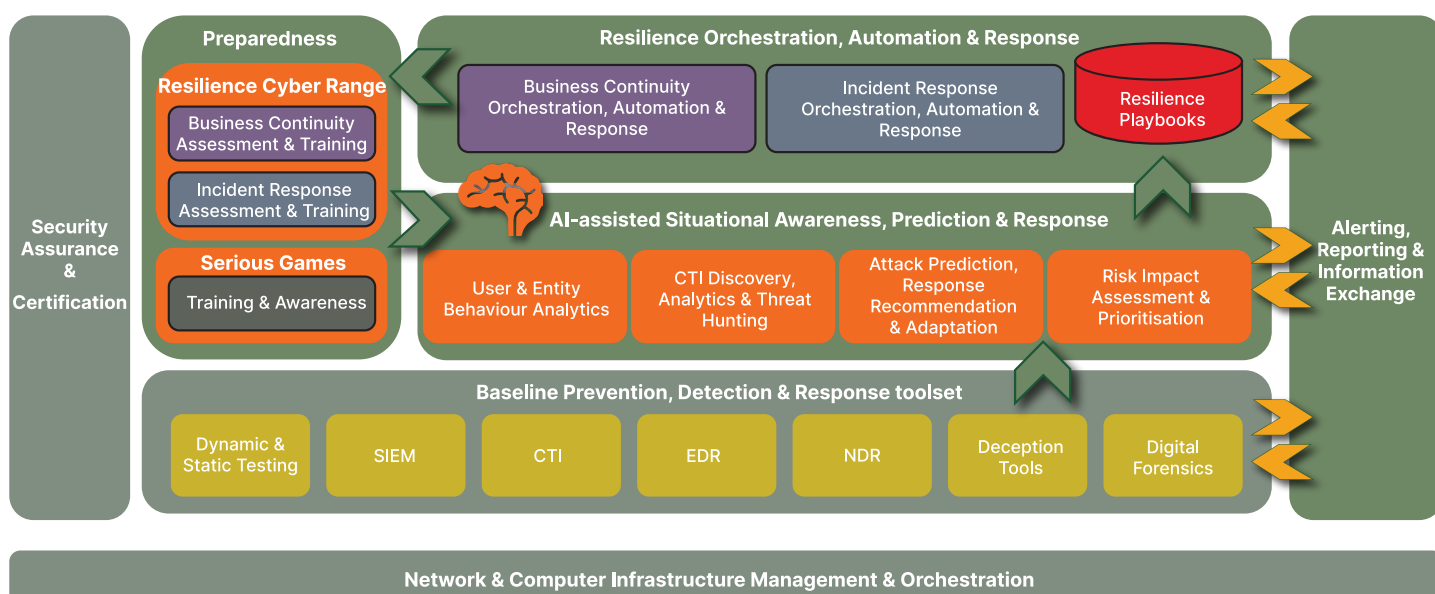
4 Preparedness

RCR: A SoTA CR, the 1st to focus on the use of a CR to assess Playbooks.

Serious Games: The 1st approach for serious games on cybersecurity improving accessibility and inclusiveness.

5 Baseline Prevention, Detection & Response toolset

MISP Security Playbooks Object Template: PHOENI2X enhanced the MISP representation schema to support security playbooks and their connection with CTI.

CACAO Layout Extension: A standardized way to visually represent cybersecurity playbooks, improving their readability, consistency, and ease of sharing.

INNOVATIONS

PHOENI2X aims at delivering
a Cyber Resilience Framework providing
Artificial Intelligence (AI) – assisted orchestration,
automation and response capabilities
for business continuity and recovery,
incident response, and information exchange,
tailored to the needs
of Operators of Essential Services (OES) and
of the EU Member State National Authorities
entrusted with cybersecurity.

Consortium

UNIVERSITY OF PATRAS ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ	Sphynx	UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH UPC	OTE GROUP OF COMPANIES
FGC Ferrocarrils de la Generalitat de Catalunya	ΔΕΗ	WORLD SENSING	AEGIS IT RESEARCH
SOCIAL ENGINEERING ACADEMY	Eunomia Ltd. Consulting Services	Atos	APIROPLUS SOLUTIONS
Nodalpoint	UiO : University of Oslo	NATIONAL CYBER SECURITY AUTHORITY GR	NATIONAL CSIRT-CY

phoeni2x.eu/ · @Phoeni2xProject · @Phoeni2xEUProject · @Phoeni2x