KEY CONCEPTS DRIVING INNOVATION IN 6G CYBERSECURITY

Xavi Masip (UPC)

HORSE Final Event, December 4th , 2025

horse-6g.eu

CONTEXTUAL CHALLENGES: THE CONTEXT

6G Architecture definition as an ongoing effort	1	No architecture, no problem to solve?
Attack surface as a yet open issue	2	New attacks to come…educated guess?
Technologies adoption (NE, AI,…)	3	Any impact to be considered???
Disaggregated ecosystem	4	Softwarized layout
Extension to “engage” other networks	5	NoN paradigm
Highly demanding services	6	Reactivity???...no way

Uncertainty

OBJECTIVE: THE FUEL

The main focus of the HORSE project is a holistic research approach aimed to design, develop and validate an autonomous, self-evolving and extendable 6G-ready architecture providing a human-centric approach to security workflows, by enabling top-down, bottom-up and end-to-end security solutions

The Concept

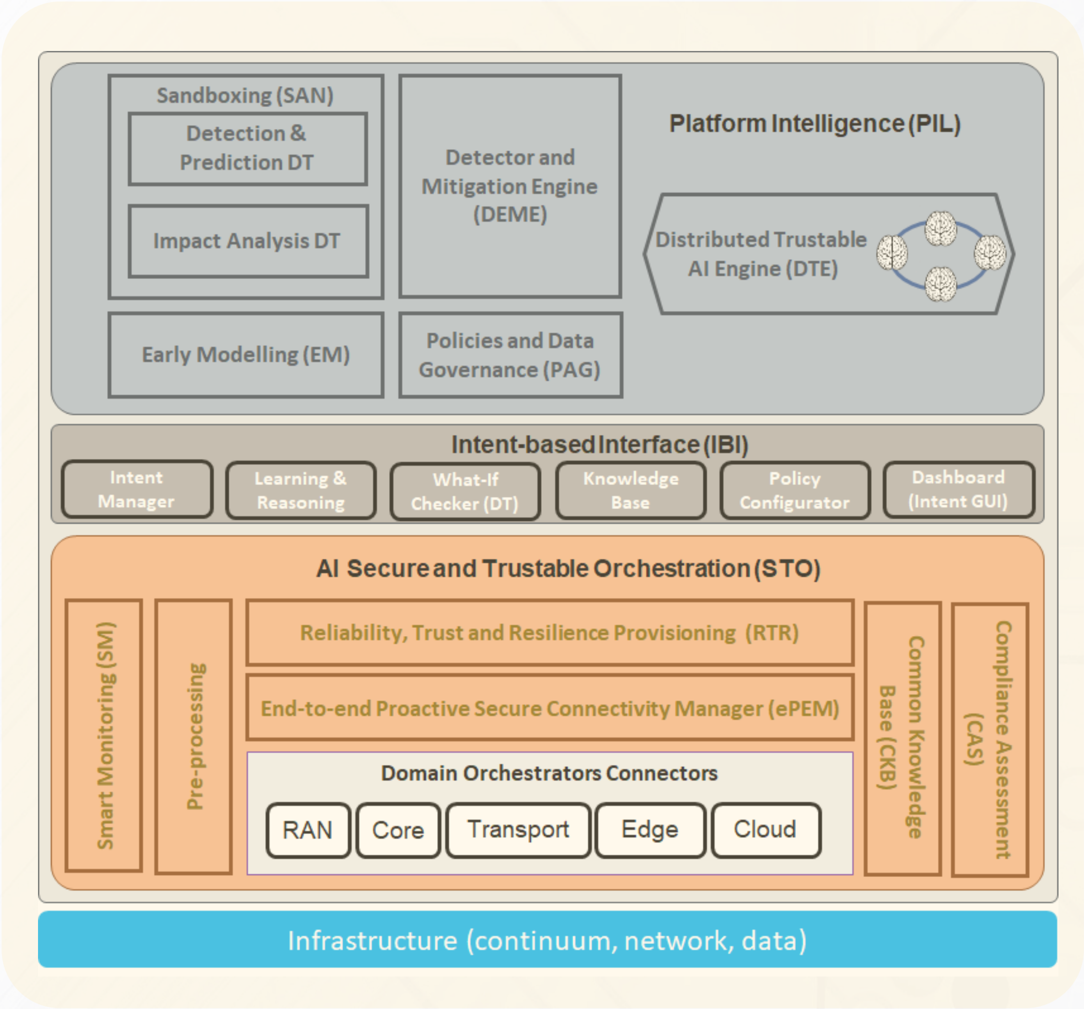
Three pivotal ingredients:
- Proactive approach based on DEME and threat modelling
- Sandbox for Impact analysis & Prediction and Prevention (What-if concept)
- Intent-based approach

The Demo

The topping:
- 2 real-world use cases
- 8 internal demos
- Three real testbeds

The Recipe

ARCHITECTURAL APPROACH: CONCEPTUAL ARCHITECTURE



Reference Architecture

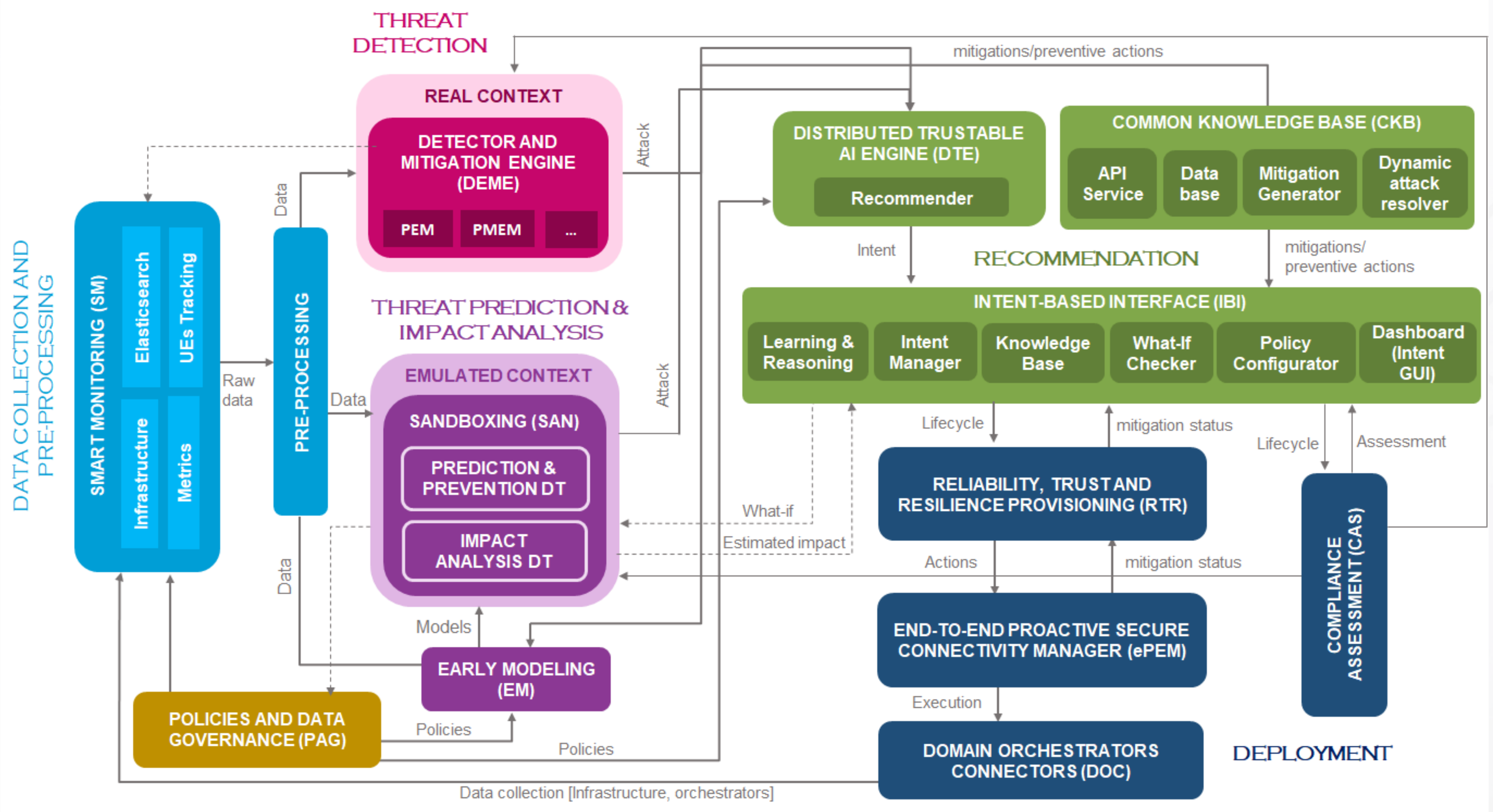
KEY BLOCKS

Platform Intelligence Layer (PIL): Featuring:
- Introduces advanced intelligence and autonomy into the system.
- Includes multiple sub-modules capable of analyzing, predicting, and optimizing network behavior

Intent-based Interface: Serving as:
- Entry point for high-level directives, allowing network administrators or intelligent software agents to express desired outcomes without needing to manage low-level configuration details.
- Its primary role is to abstract and simplify network control through intent-driven interactions.

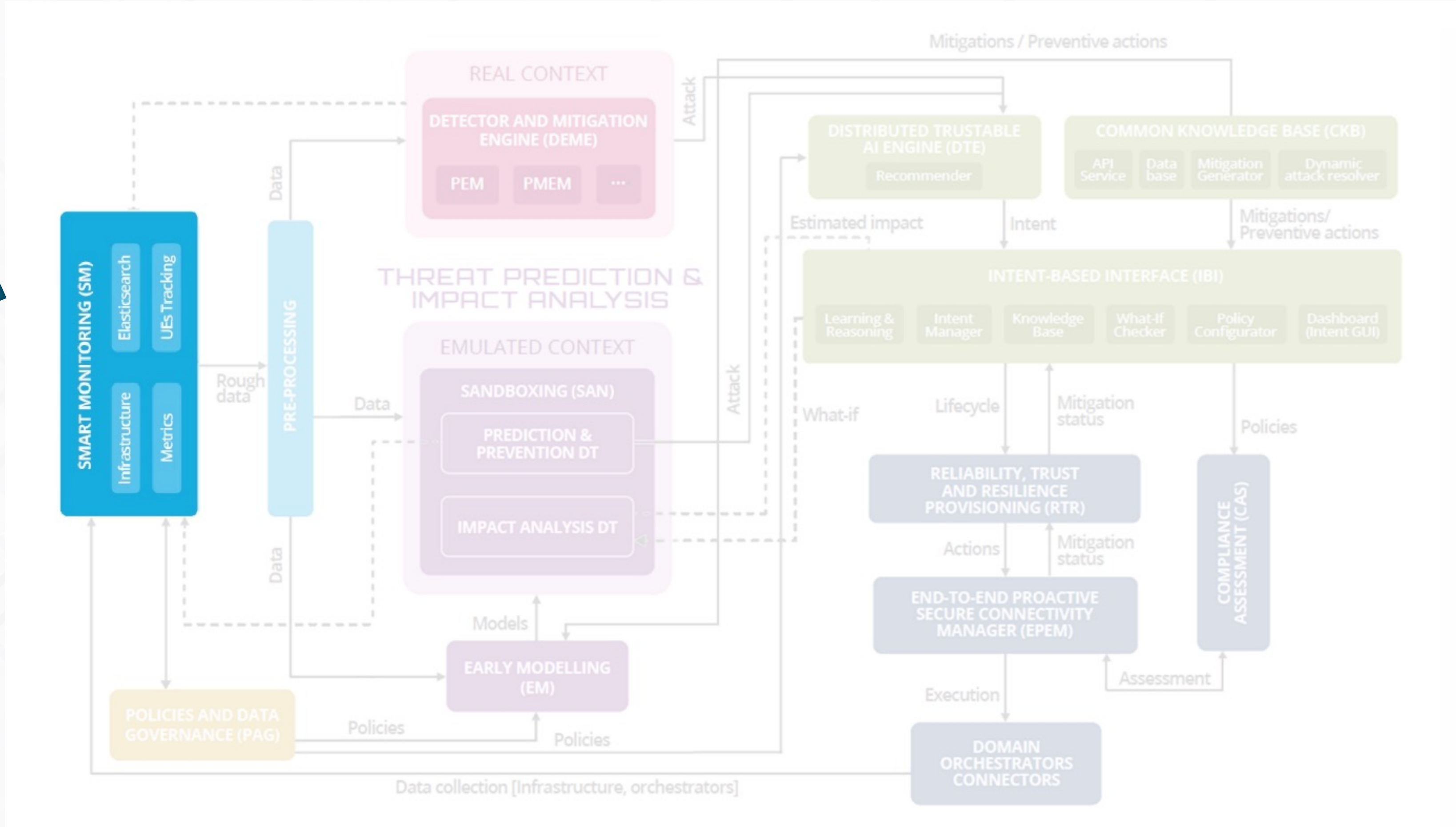
AI Secure and Trustable Orchestration (STO) : Responsible for:
- Dependable orchestration of network resources
- Ensures that the intents expressed via the IBI are correctly interpreted and translated into executable actions
- Enforcing the corresponding policies while maintaining system reliability and trustworthiness

ARCHITECTURAL APPROACH: FUNCTIONAL ARCHITECTURE



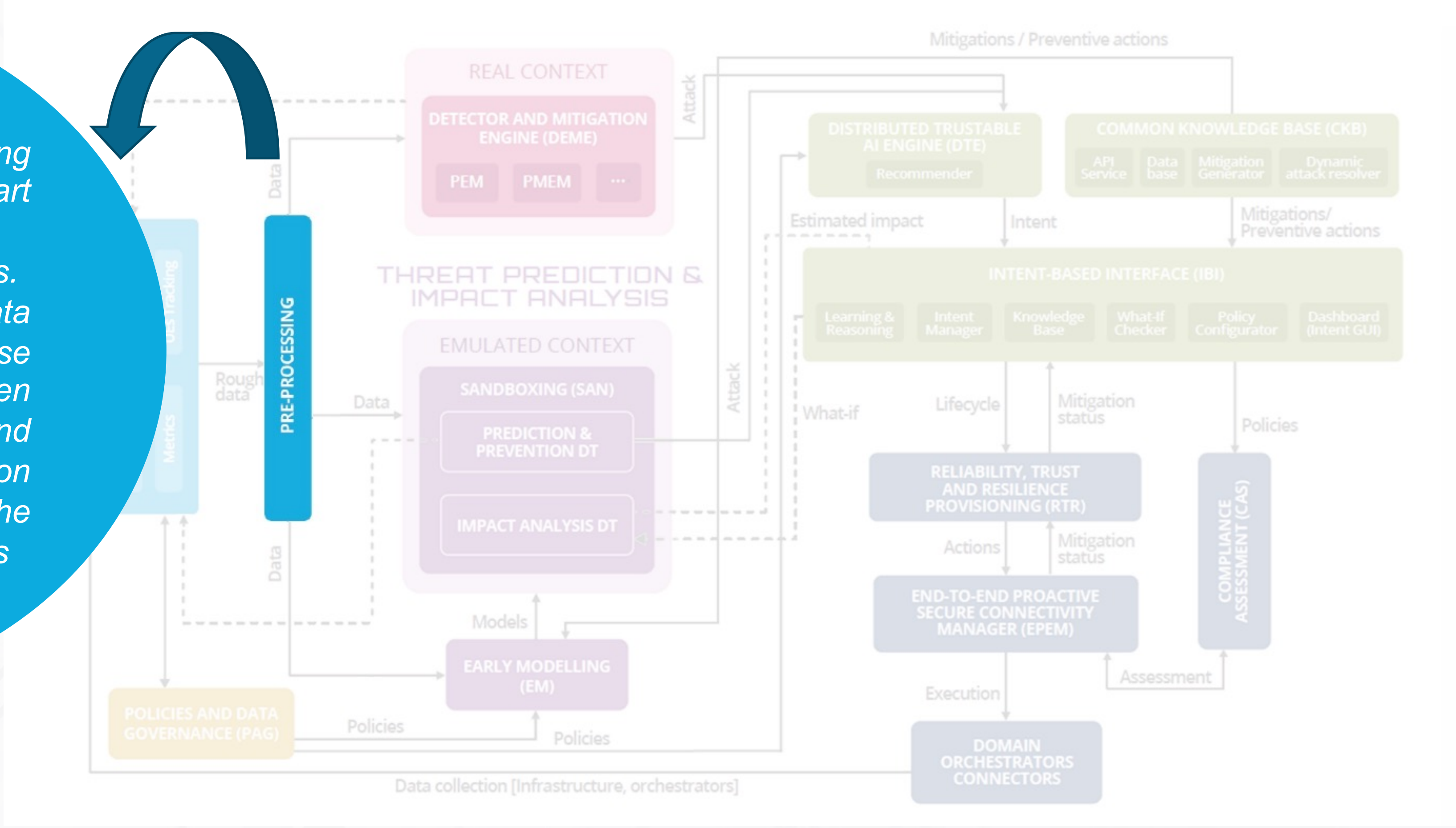
SMART MONITORING (SM)

Central observability hub, with enhanced ingestion, indexing, and fine-grained access control using ElasticSearch



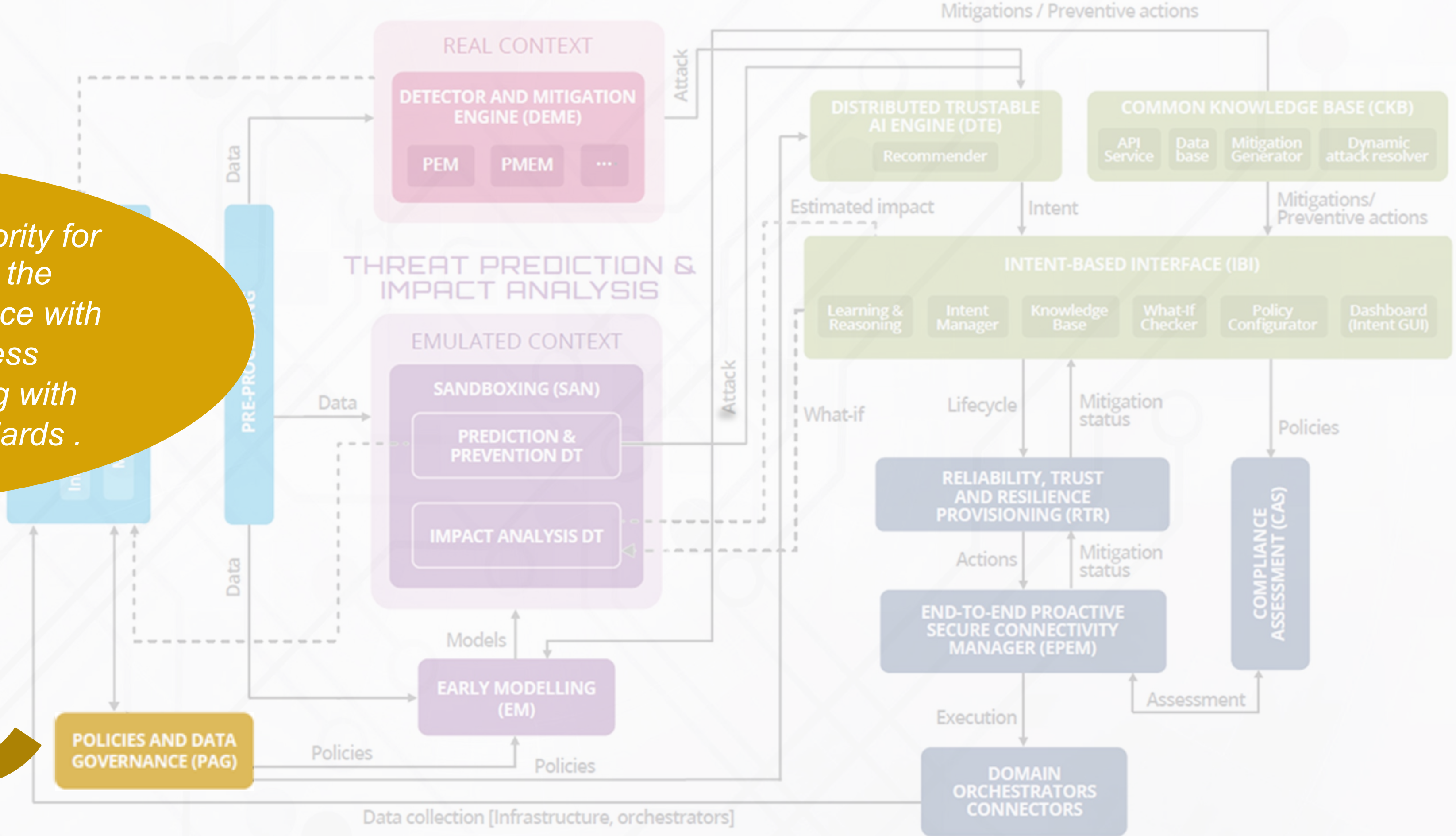
PRE-PROCESSING

- *Harmonizing and standardizing raw data from the Smart Monitoring (SM)*
- *Subsequent analytical processes.*
- *Responsible for extracting data from the Elasticsearch database of the SM component and then pre-processing it to clean and restructure the information according to the needs of the consuming software components*

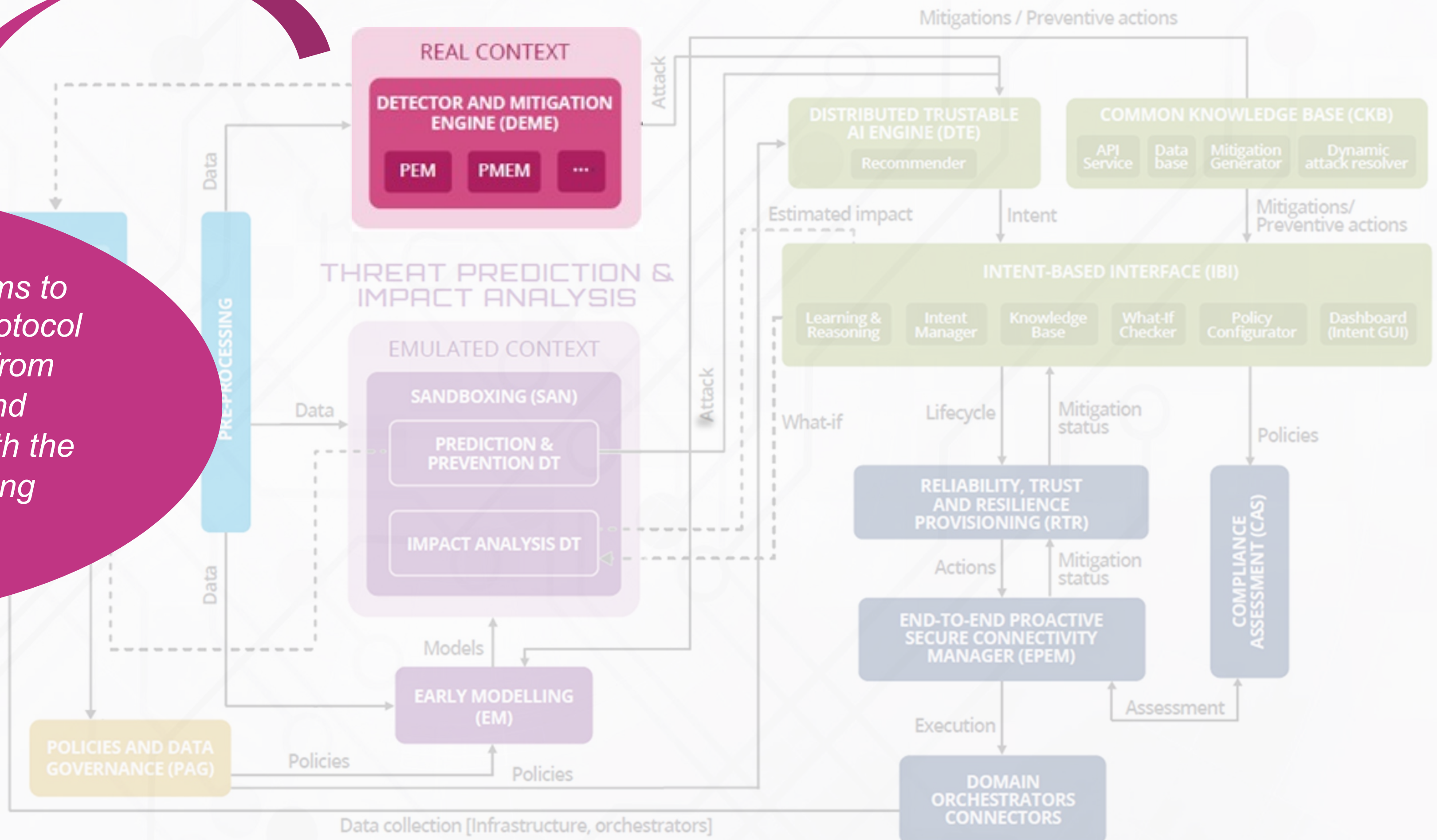


POLICIES AND DATA GOVERNANCE (PAG)

It functions as a central authority for data management across the platform. It ensures compliance with privacy, quality, and access requirements, while aligning with regulatory and ethical standards .

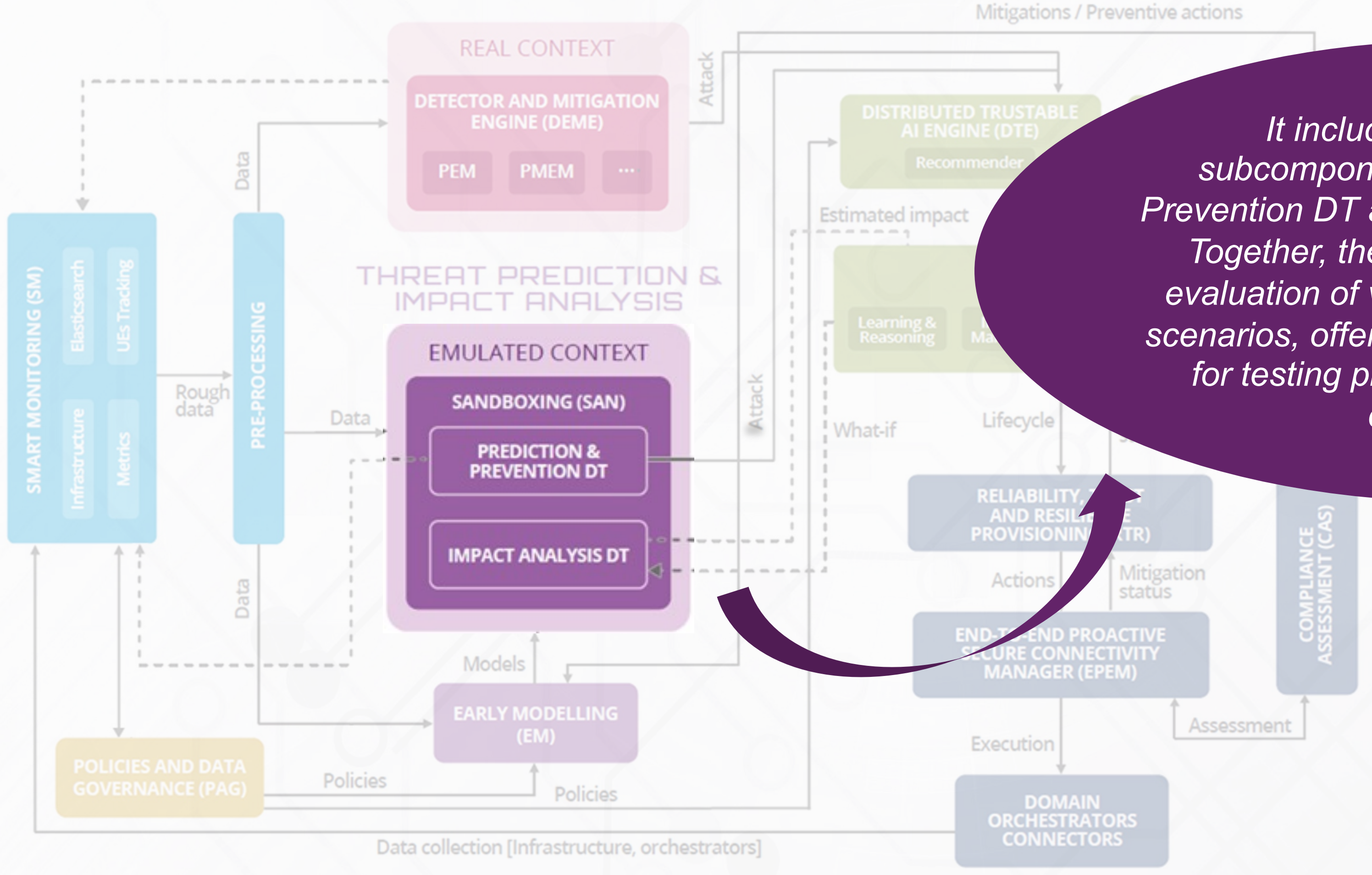


DETECTOR AND MITIGATION ENGINE (DEME)



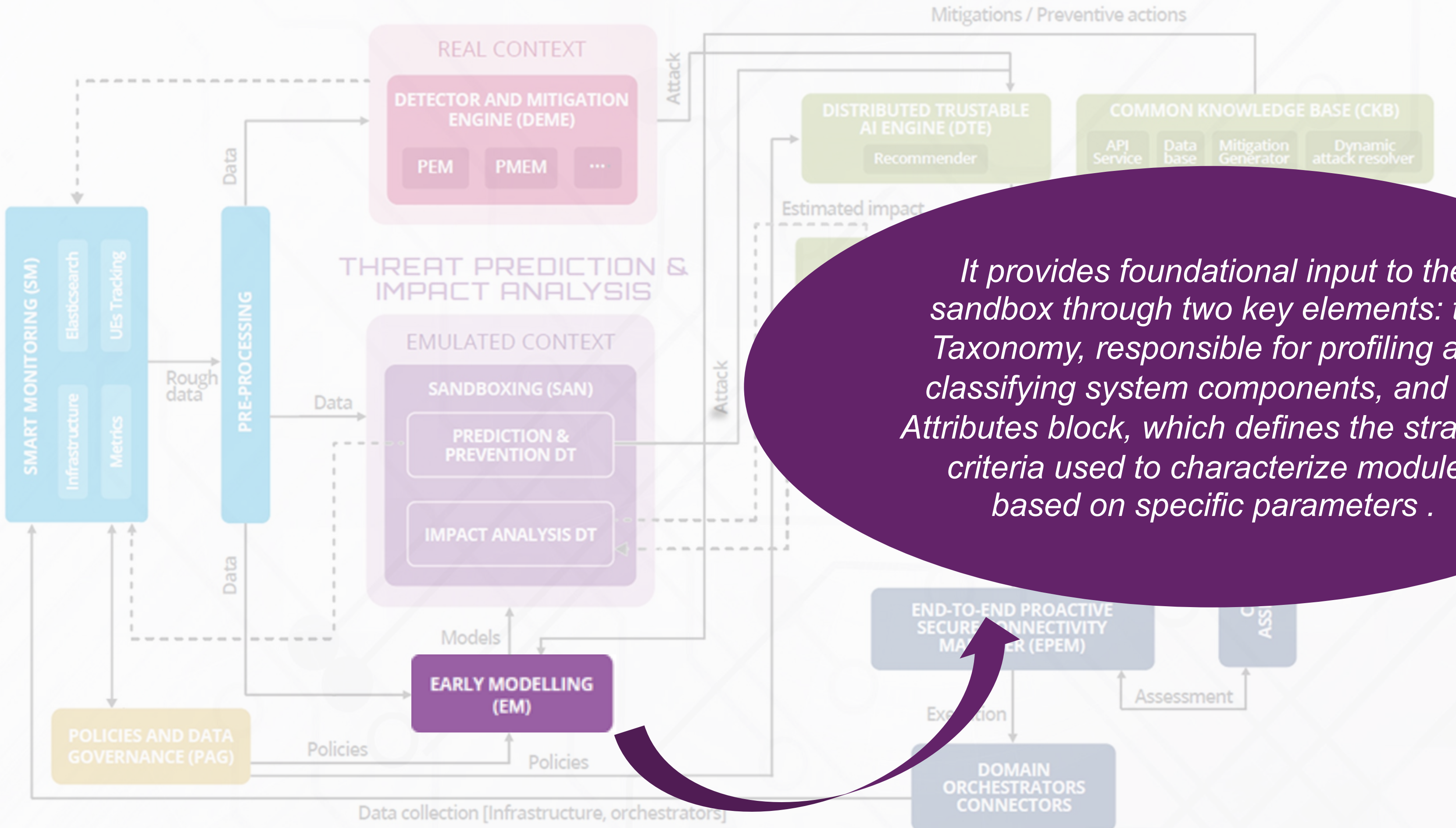
It employs specialized algorithms to analyze network parameters, protocol headers, and real-time traffic from various network elements and virtualized functions (VNFs), with the goal of detecting and mitigating potential threats.

SANDBOXING (SAN)



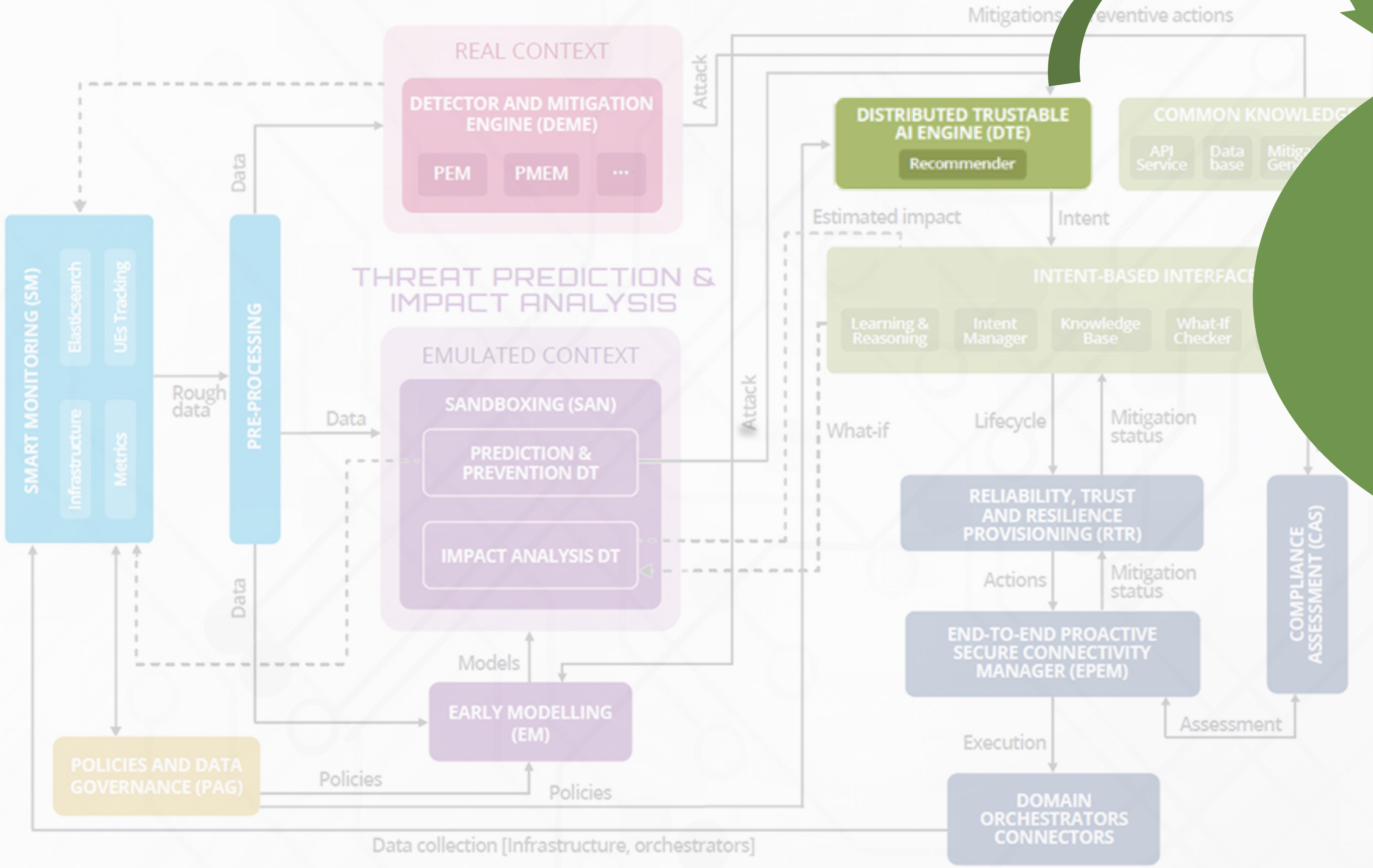
It includes two Digital Twin subcomponents: the Prediction and Prevention DT and the Impact Analysis DT. Together, they enable simulation and evaluation of various configurations and scenarios, offering a dynamic environment for testing platform behaviour before deployment .

EARLY MODELLING (EM)



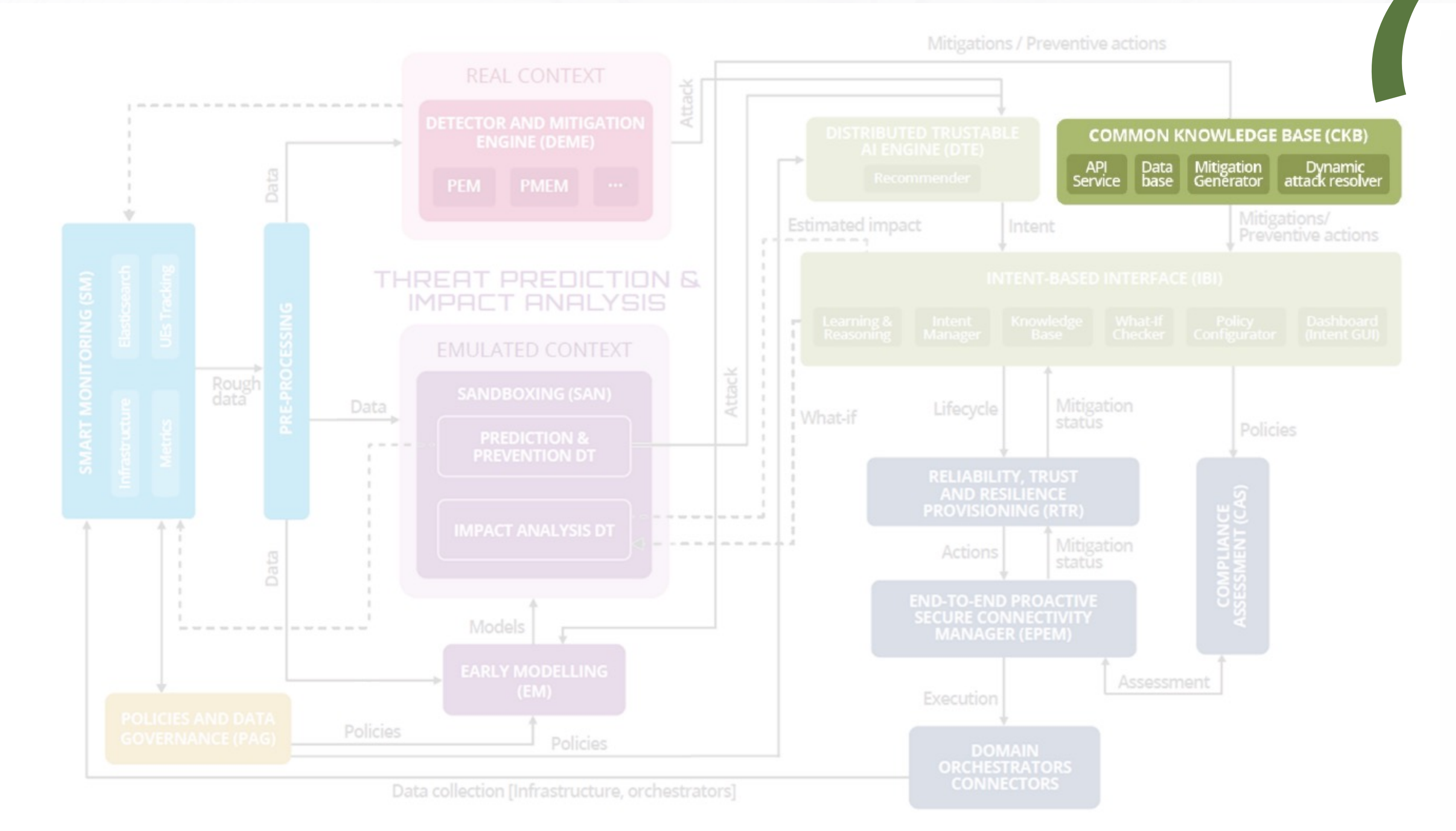
It provides foundational input to the sandbox through two key elements: the Taxonomy, responsible for profiling and classifying system components, and the Attributes block, which defines the strategic criteria used to characterize modules based on specific parameters .

DISTRIBUTED TRUSTABLE AI ENGINE (DTE)

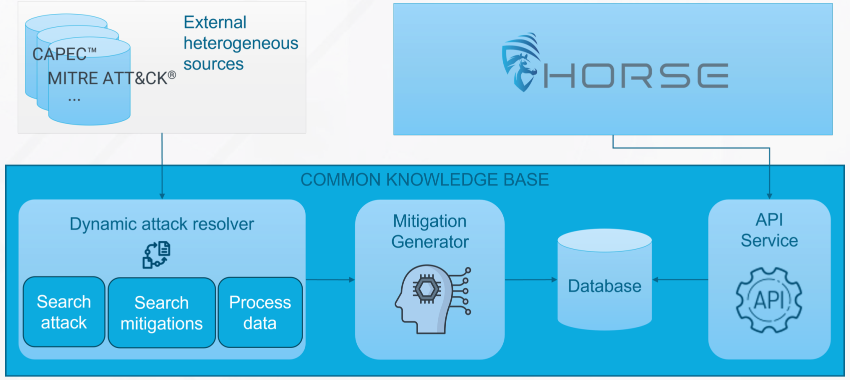


Collects and processes data from multiple sources using machine learning and AI techniques to derive security policies while ensuring data privacy. It also supports data pre-processing for model training and integrates with other intelligence components in the platform.

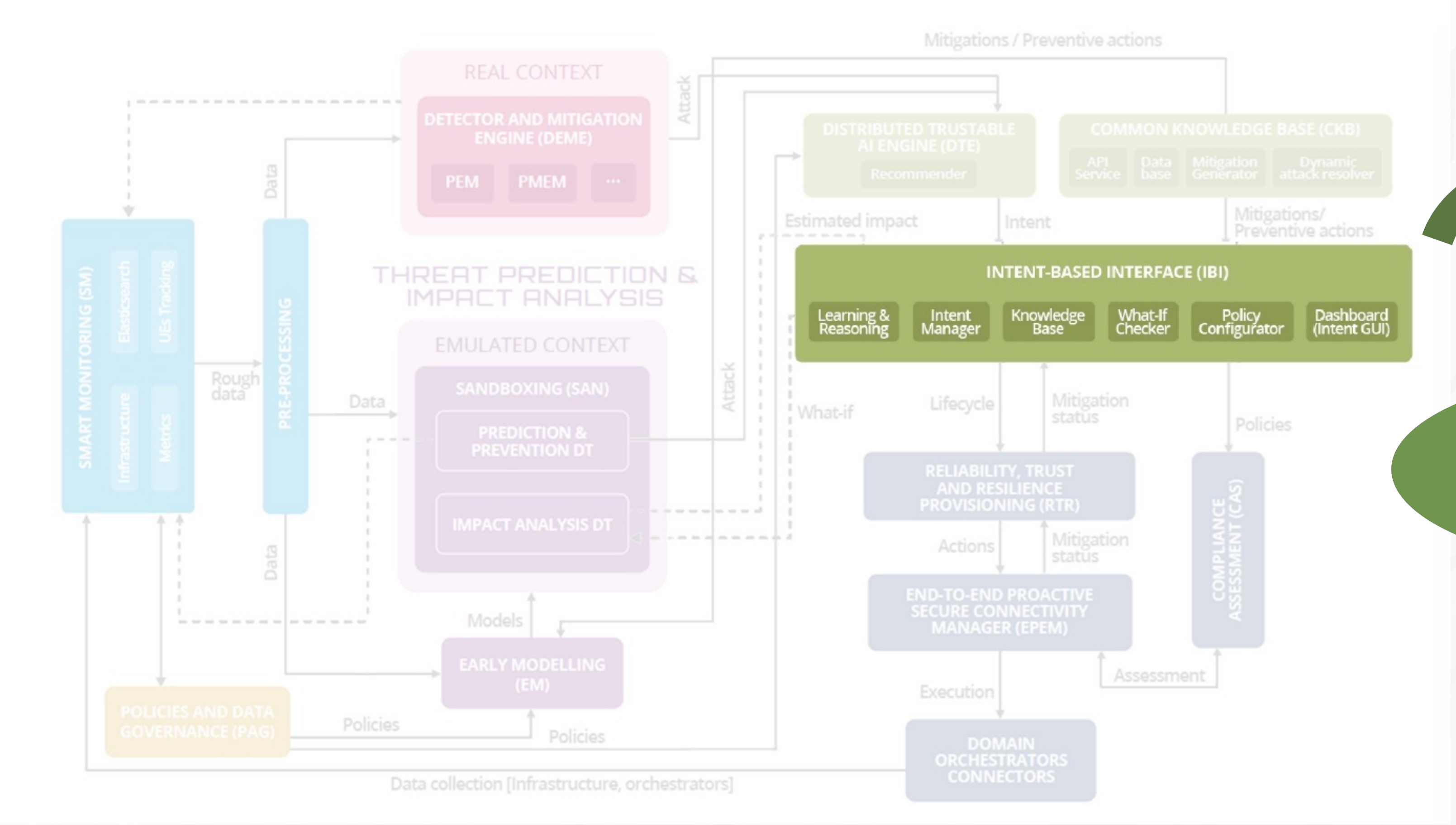
COMMON KNOWLEDGE BASE (CKB)



Centralized threat and mitigation intelligence, using Generative AI and LLMs for dynamic updates and prioritization.

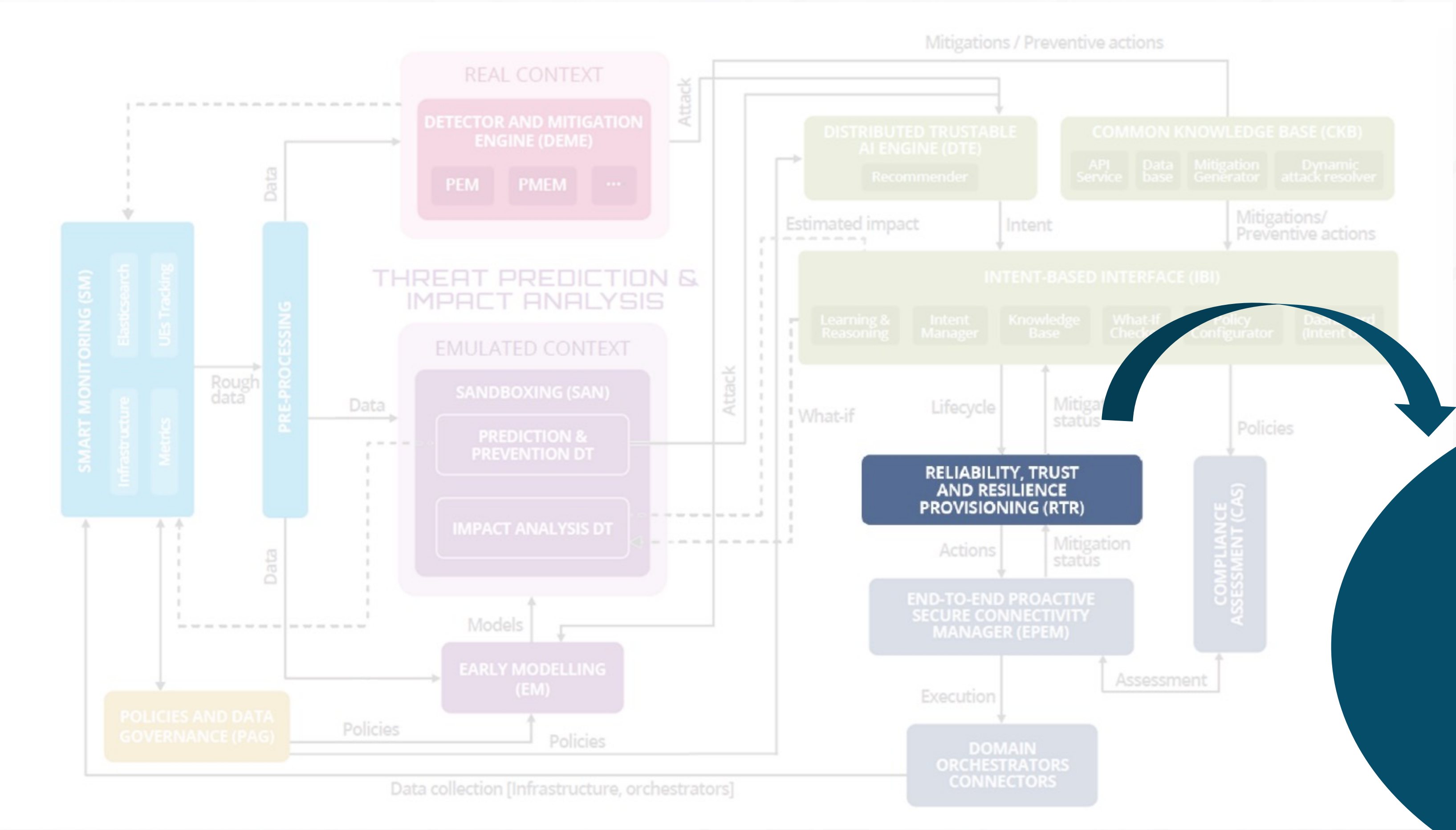


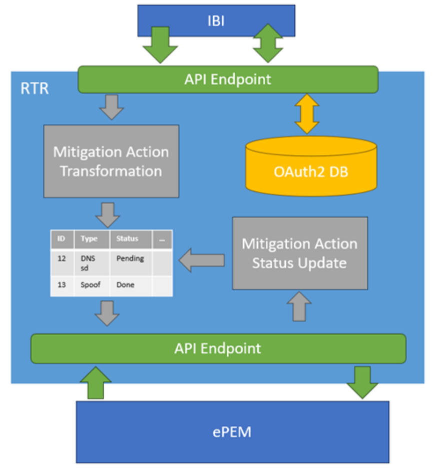
INTENT-BASED INTERFACE (IBI)



It receives intents from human operators that are translated into network configurations.

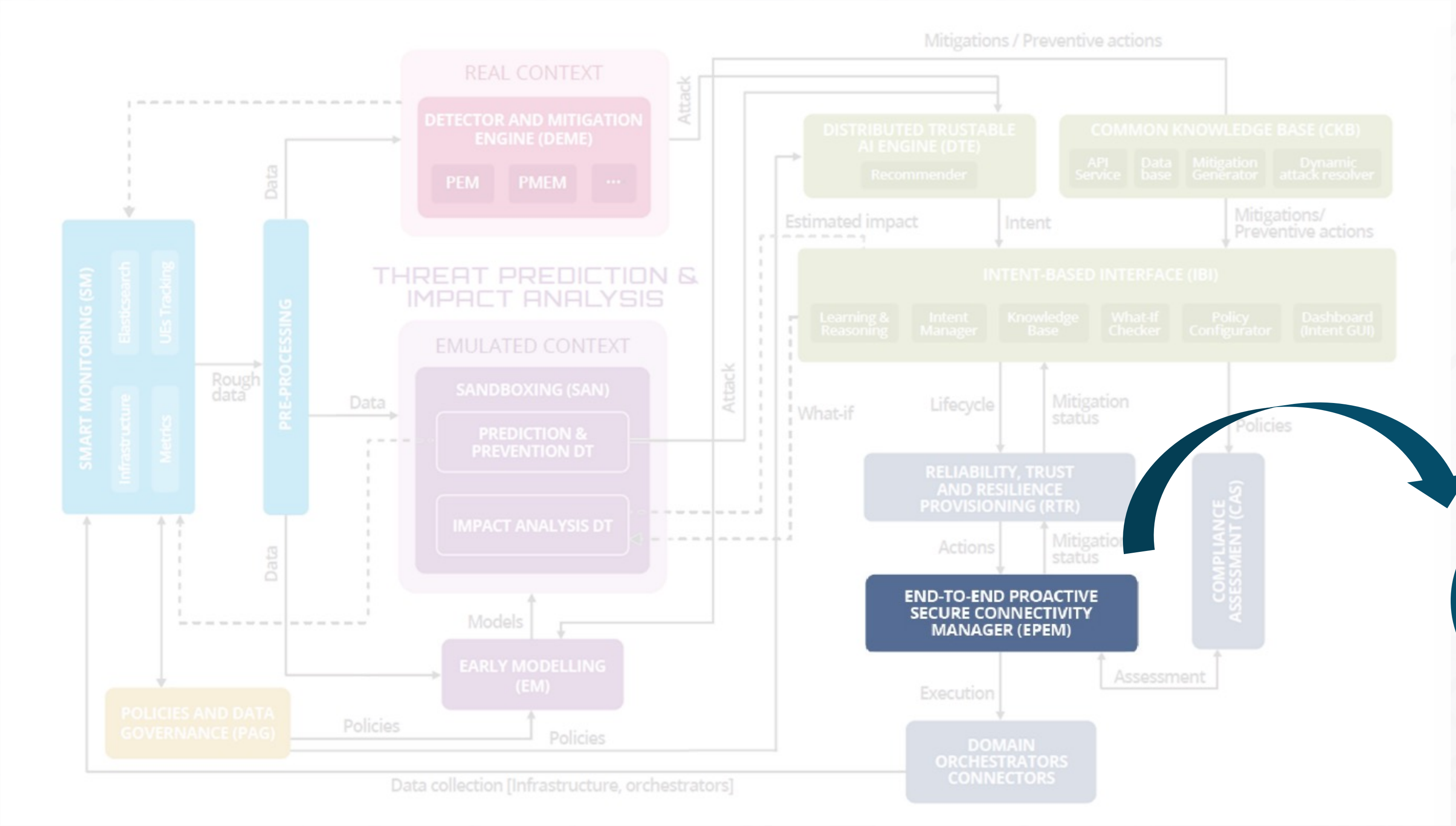
RELIABILITY, TRUST AND RESILIENCE PROVISIONING (RTR)





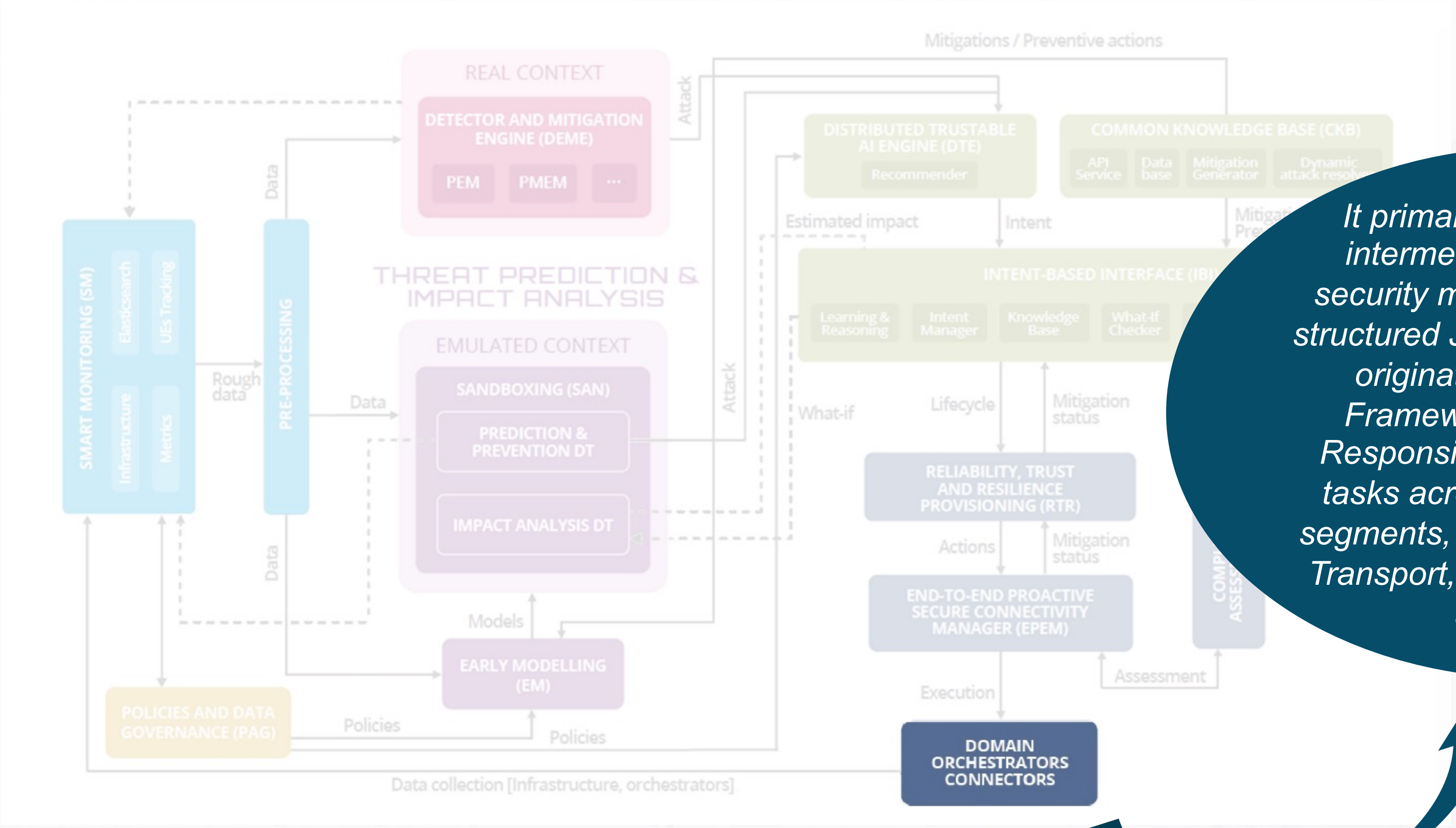
Its core function involves processing high-level security intents originating from the Intent-Based Interface (IBI) and translating these into actionable mitigation measures, which are subsequently forwarded to the End-to-End Proactive Secure Connectivity Manager (ePEM).

E2E PROACTIVE SECURE CONECTIVITY MANAGER (EPEM)



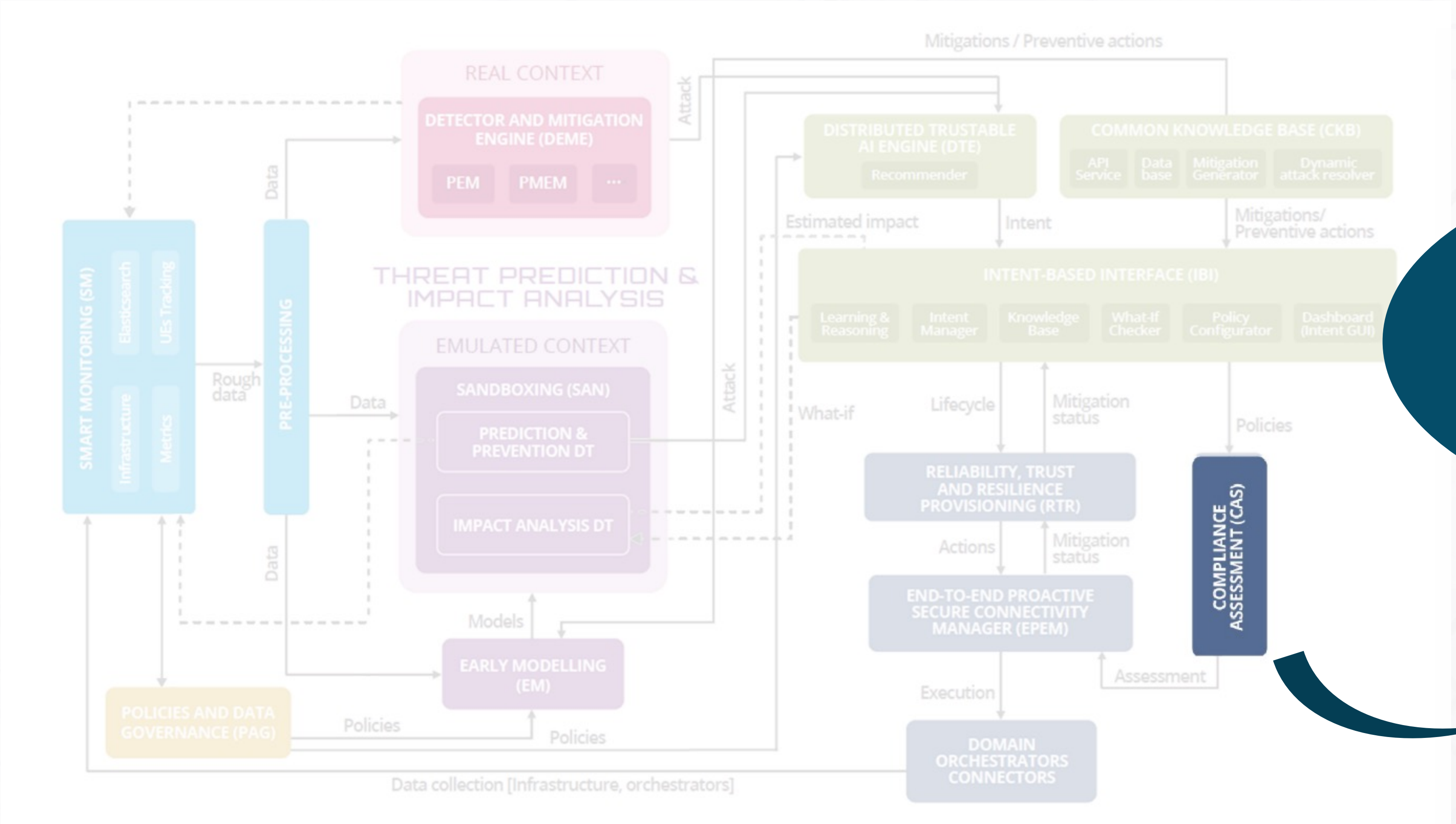
Orchestrating actions and providing observability over various components that constitute the end-to-end services secured within the HORSE security perimeter

DOMAIN CONNECTORS (DOC)



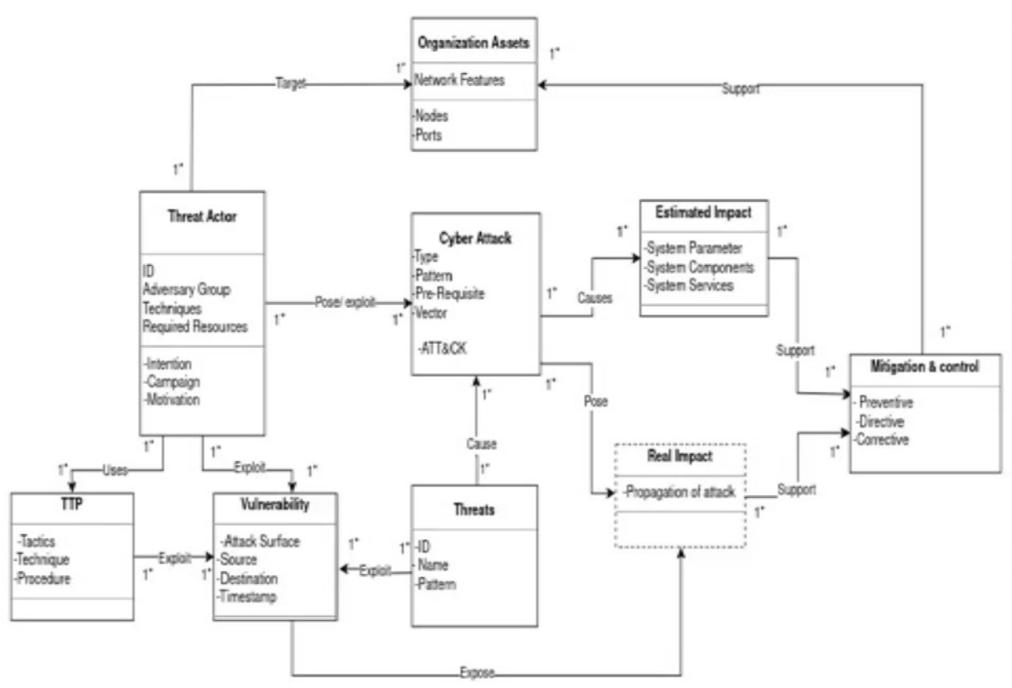
It primarily functions as an intermediary that receives security mitigation actions in a structured JSON format, typically originating from the RTR Framework via the ePEM. Responsible for orchestrating tasks across diverse network segments, including RAN, Core, Transport, Edge (near and far), and Cloud.

COMPLIANCE ASSESSMENT (CAS)



It aims to ensure all HORSE actions comply with predefined security and privacy policies. It also verifies that decisions from the Trustable AI engine align with regulations.

KEY CONCEPTS - I: PROACTIVE APPROACH



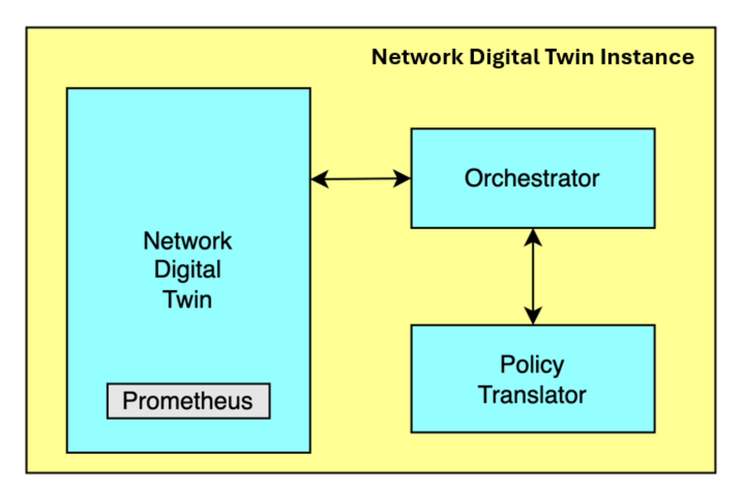
Threat Modeling

Driven by the Threat Detector and Mitigation Engine (DEME)

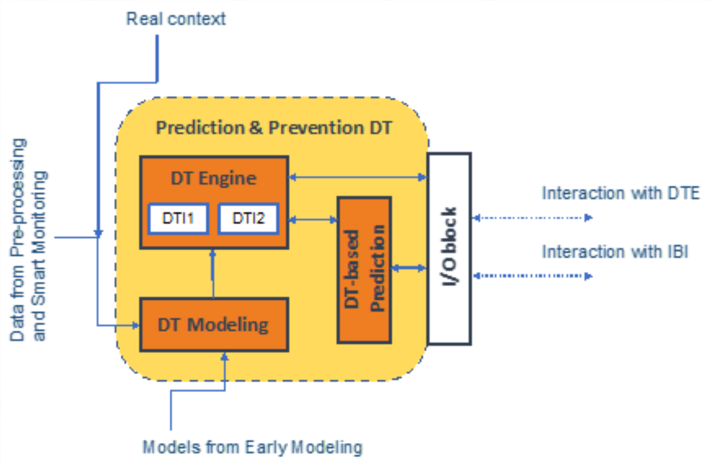
- It integrates ML, cybersecurity and Digital Twins, enhancing overall detection and response capabilities,
- The system allows attacks to be identified the moment a deviation from expected behavior occurs, without predefined thresholds to be crossed.
- Detection sources are strategically selected as close as possible to the root of the potential threat, significantly reducing detection latency.
- It includes both cutting-edge algorithms and custom-developed HORSE algorithms,
- It overcomes siloization, by deploying multiple specialized detectors in parallel, whose outputs are then aggregated and correlated in downstream stages.
- It assigns a risk probability or confidence score to each detection event, allowing for a more adaptive and intelligent cybersecurity response strategy.

KEY CONCEPTS - II: WHAT-IF + NDT + COMPLIANCE ASSESSMENT

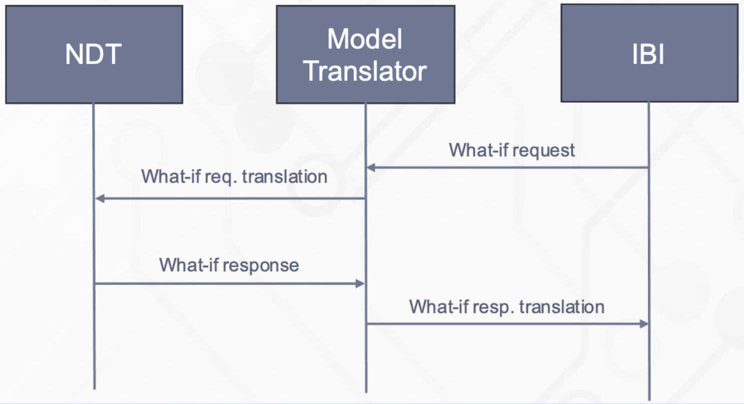
Impact Analysis Architecture



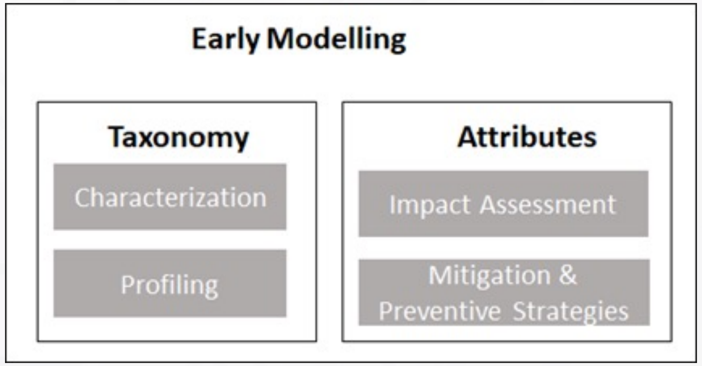
Predictive and Preventive Analysis Architecture



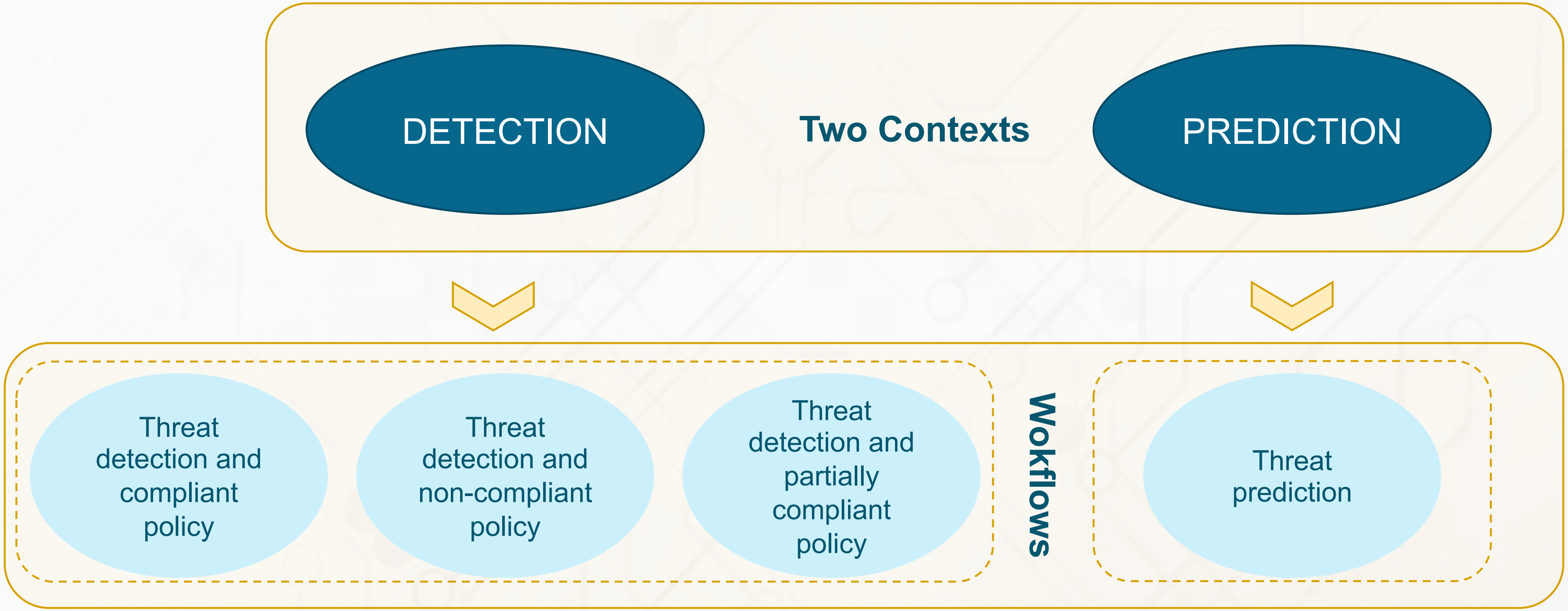
Workflow



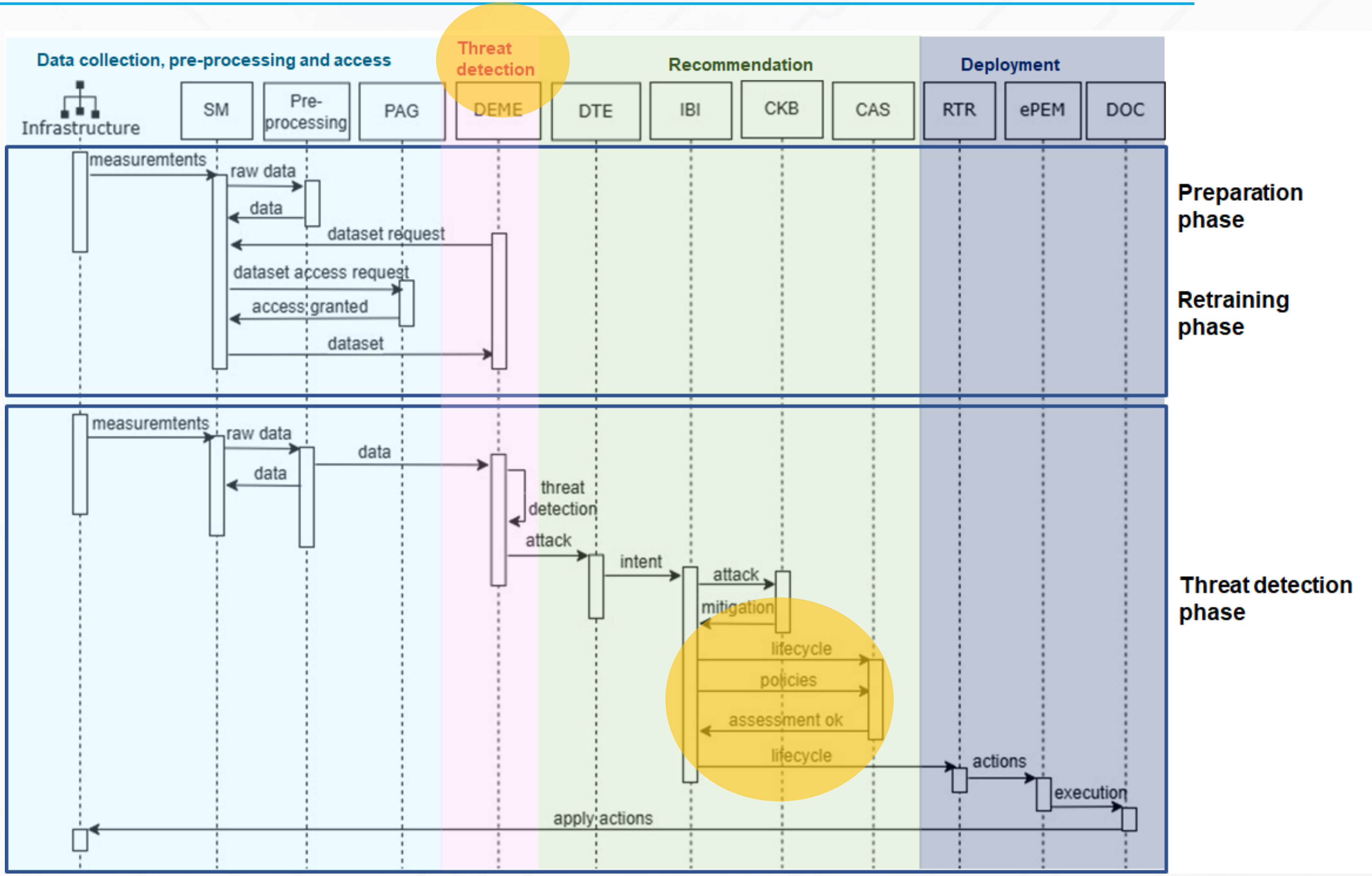
Early Modelling



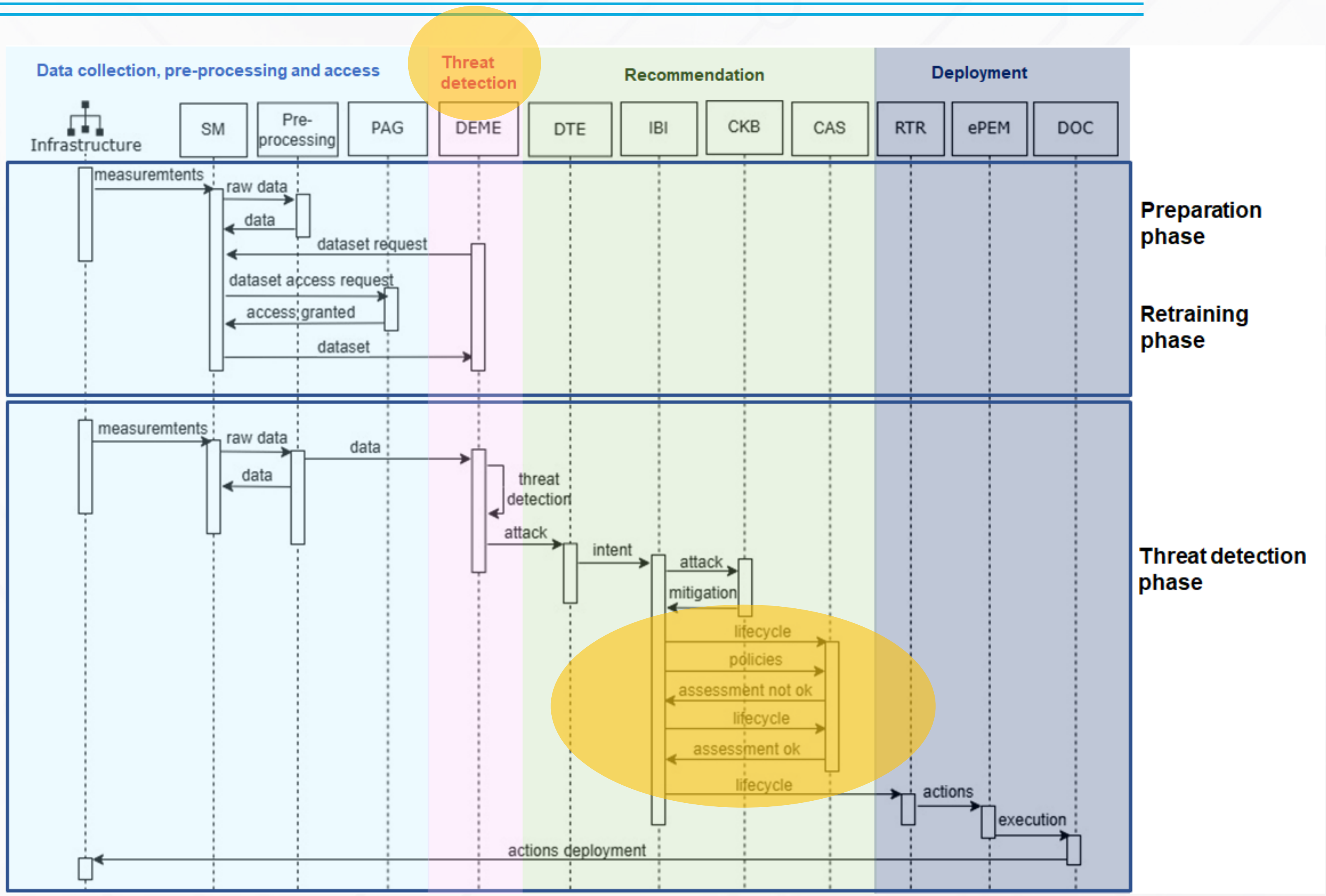
CANONICAL WORKFLOWS SCENARIOS



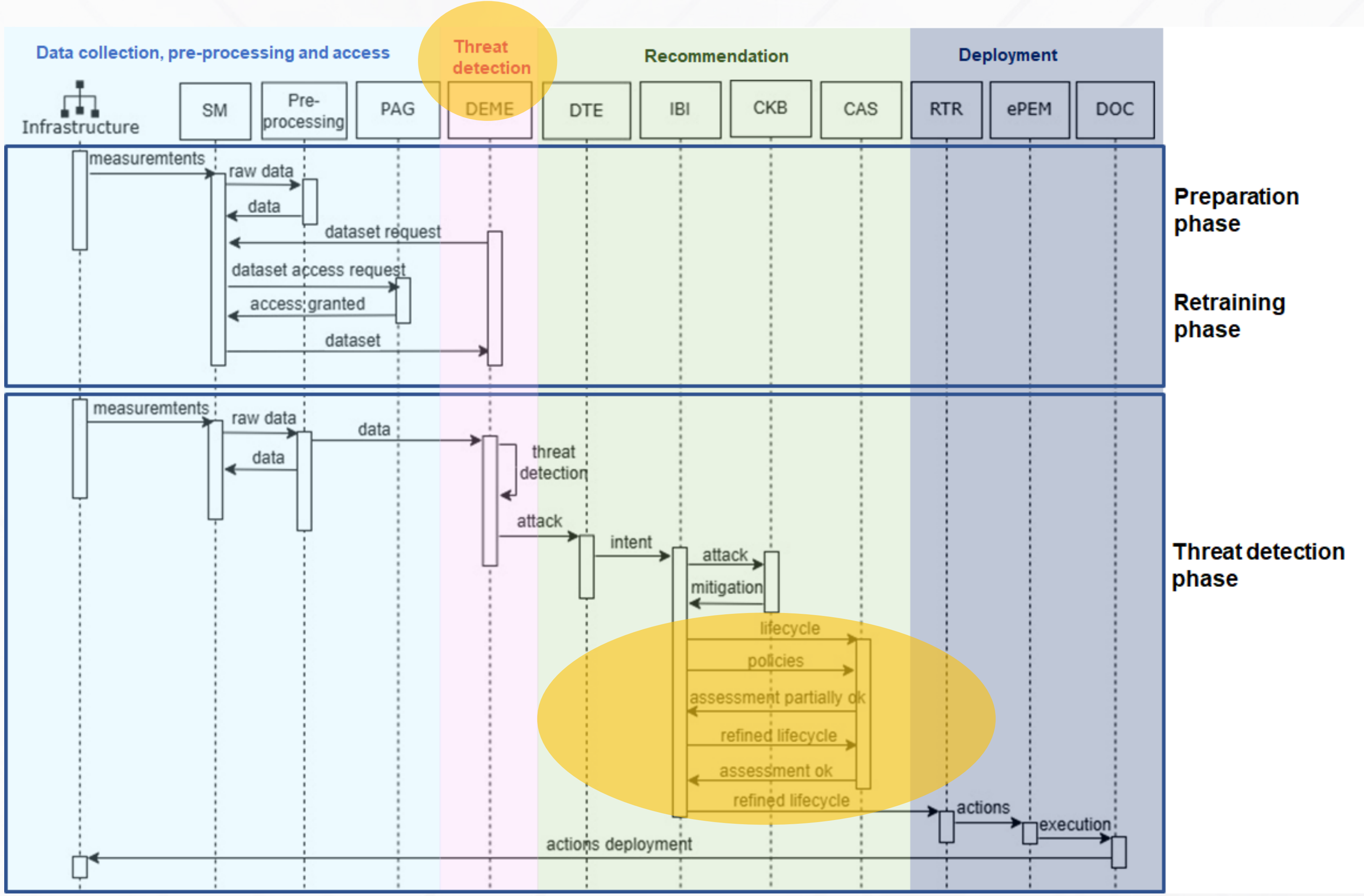
CANONICAL WORKFLOWS: THREAT DETECTION & COMPLIANT POLICY



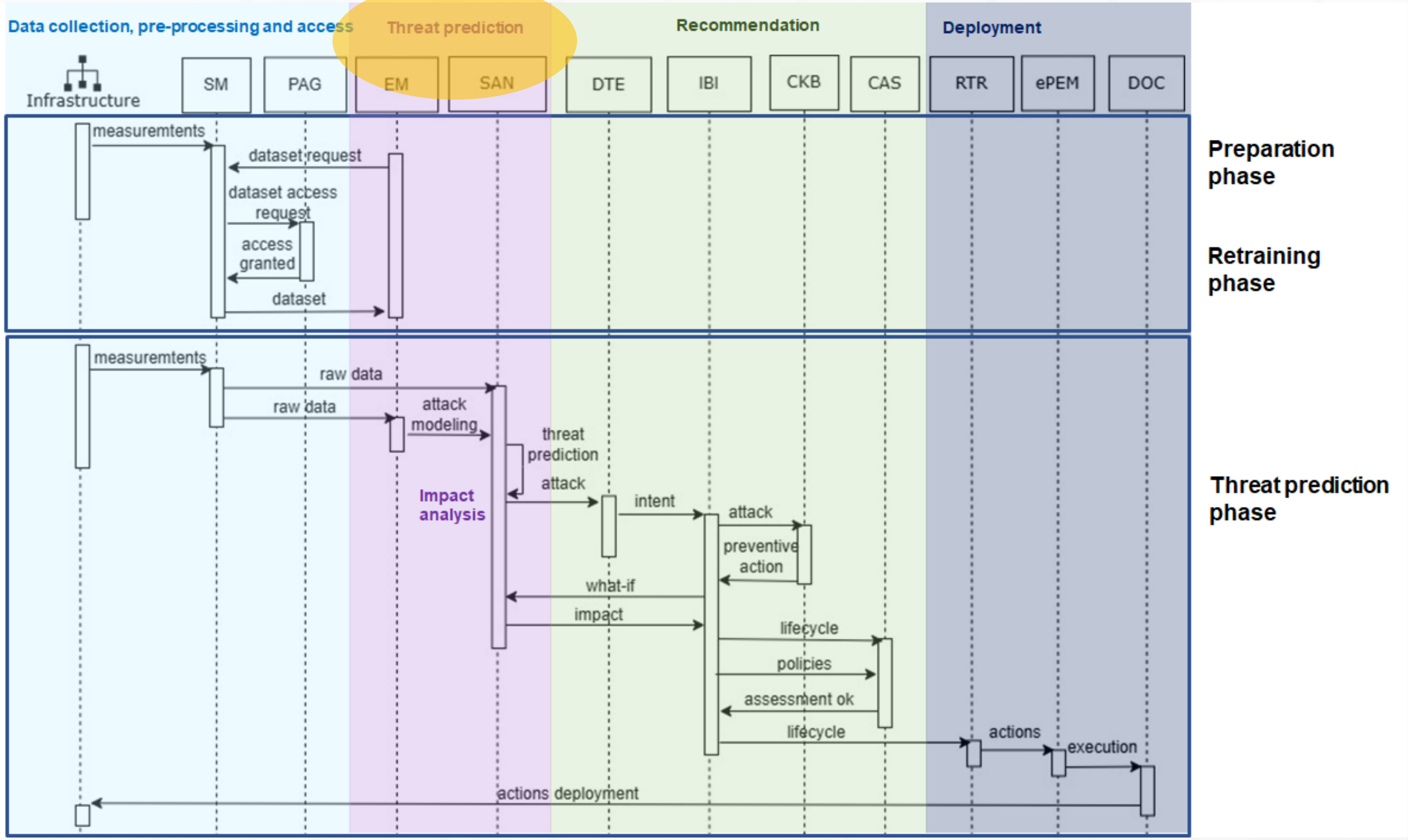
CANONICAL WORKFLOWS: THREAT DETECTION & NON COMPLIANT POLICY



CANONICAL WORKFLOWS: THREAT DETECTION & PARTIALLY COMPLIANT



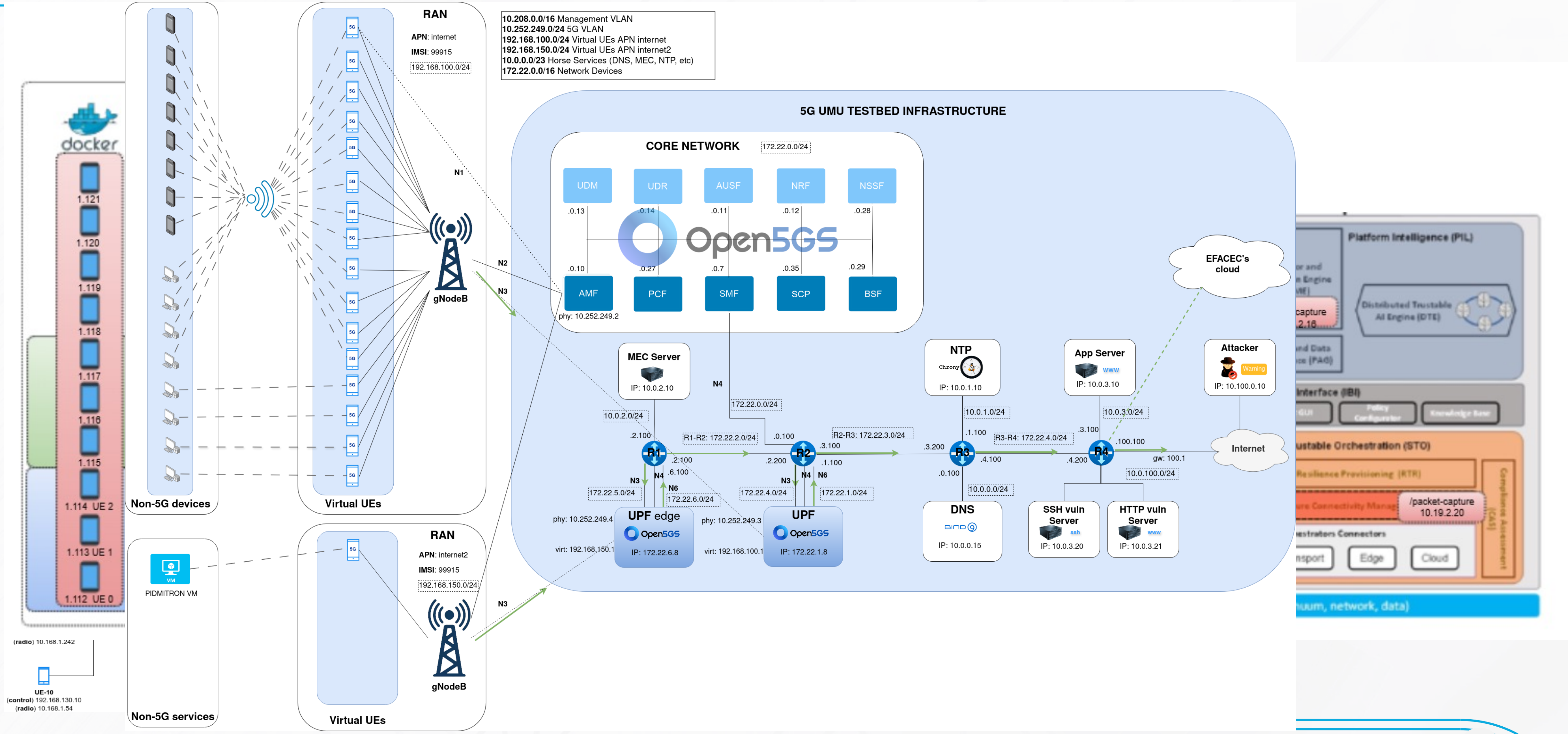
CANONICAL WORKFLOWS: THREAT PREDICTION



DEMO CONTEXT

0.	Hello-world (components interface test)	**UPC**
1.	Detect an NTP DDoS (NTP amplification attack)	**E///,** CNIT
2.	Predict&Impact Analysis a DNS DDoS (DNS amplification attack)	**UMU (TID),** UPC, CNIT
3.	Predict&Impact&Compliance a DNS DDoS (DNS amplification attack)	**UMU (TID),** UPC, CNIT
4.	Detect DT data poisoning	**CNIT**
5.	Multidomain DDoS DNS	**UPC**, CNIT (TID)
6.	MitM on IBI intents	**TUBS**
7.	API and Network Exposure	**E///,** CNIT
8.	Attack on signaling PFCP traffic	**NKUA**, UPC, CNIT, TID
9.	EFACEC Use Case	**EFACEC,** UPC, CNIT, UMU
10.	HOLO Use Case	**HOLO**, CNIT

TESTBEDS: CNIT, UPC & UMU



SO…IN SHORT

- Proactive Approach
- What-if (EM+SAN)
- Early detection/prediction
- Credible validation strategy

THANK YOU FOR YOUR ATTENTION

horse-6g.eu

HORSE project has received funding from the Horizon Europe research and innovation programme under grant agreement N° 101096342

THANK YOU FOR YOUR ATTENTION

horse-6g.eu

HORSE project has received funding from the Horizon Europe research and innovation programme under grant agreement N° 101096342

PROJECT CONSORTIUM