



A Certification-Oriented Cyber Range Based on a Digital Twin

Ahmed Bokri¹ Khaled Rahal^{1 2} Arbia Riahi¹ Wim Mees¹
¹Royal Military Academy, Brussels | ²Université Libre de Bruxelles



1- Motivation and Objectives

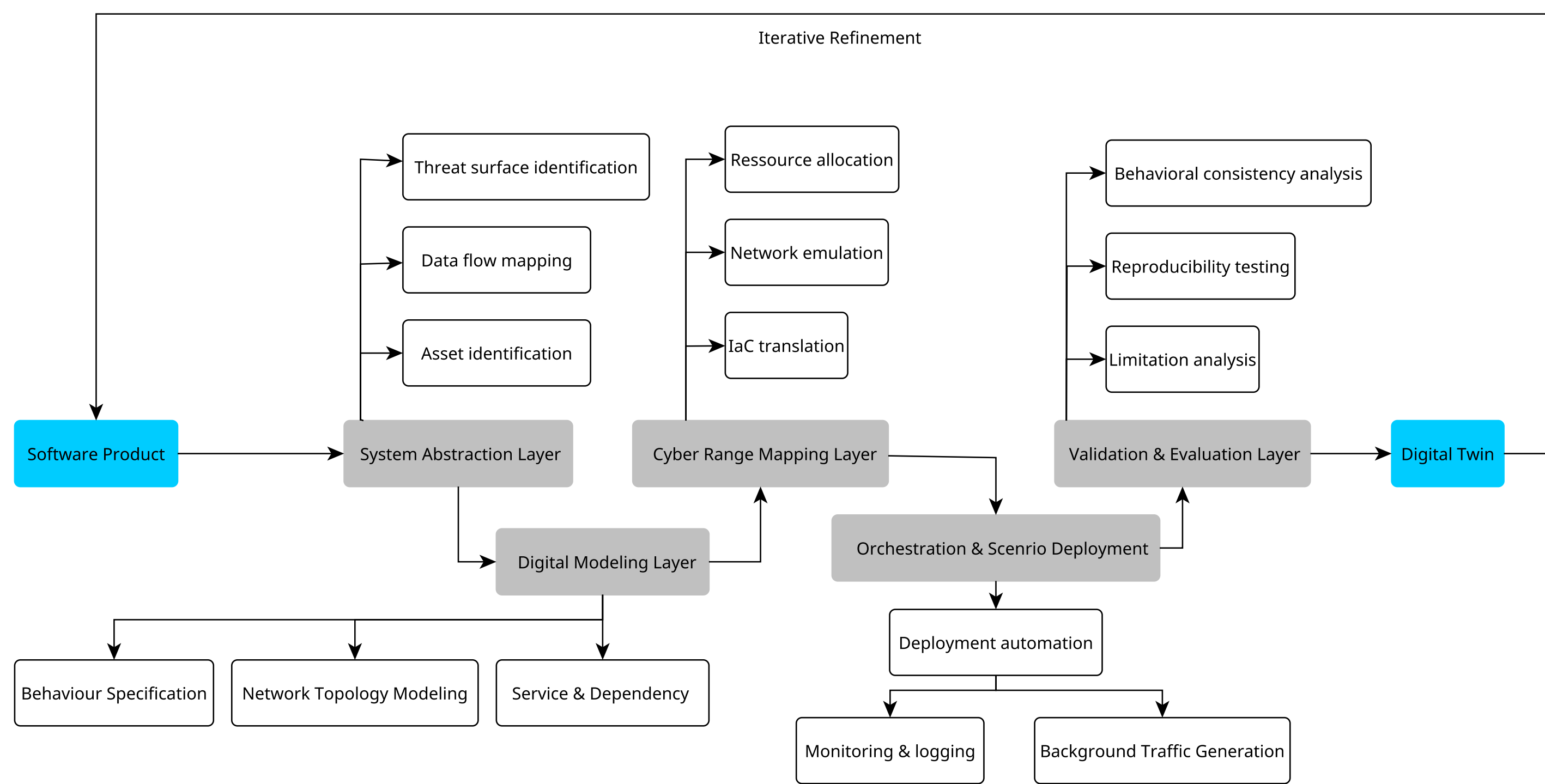
AMC3 context: Digital Twin-based support for cybersecurity certification of defense software [1].

MASFAD use case: a military multi-agent system for APT detection requiring controlled, repeatable, observable, and traceable assessment conditions [2].

Constraint: production infrastructures are unsuitable due to confidentiality, availability, and safety risks.

Objective: build a reproducible **KYPO-based Digital Twin** to evaluate MASFAD as the **TOE** under declared operational assumptions [3].

2- Layered Methodology



Construction layers:

Abstraction: assets, data flows, threat surface;

Modeling: topology, services, dependencies;

Mapping: cyber-range resources, networks, IaC artifacts;

Orchestration: deployment, logging, traffic generation;

Validation: reproducibility and behavioral consistency.

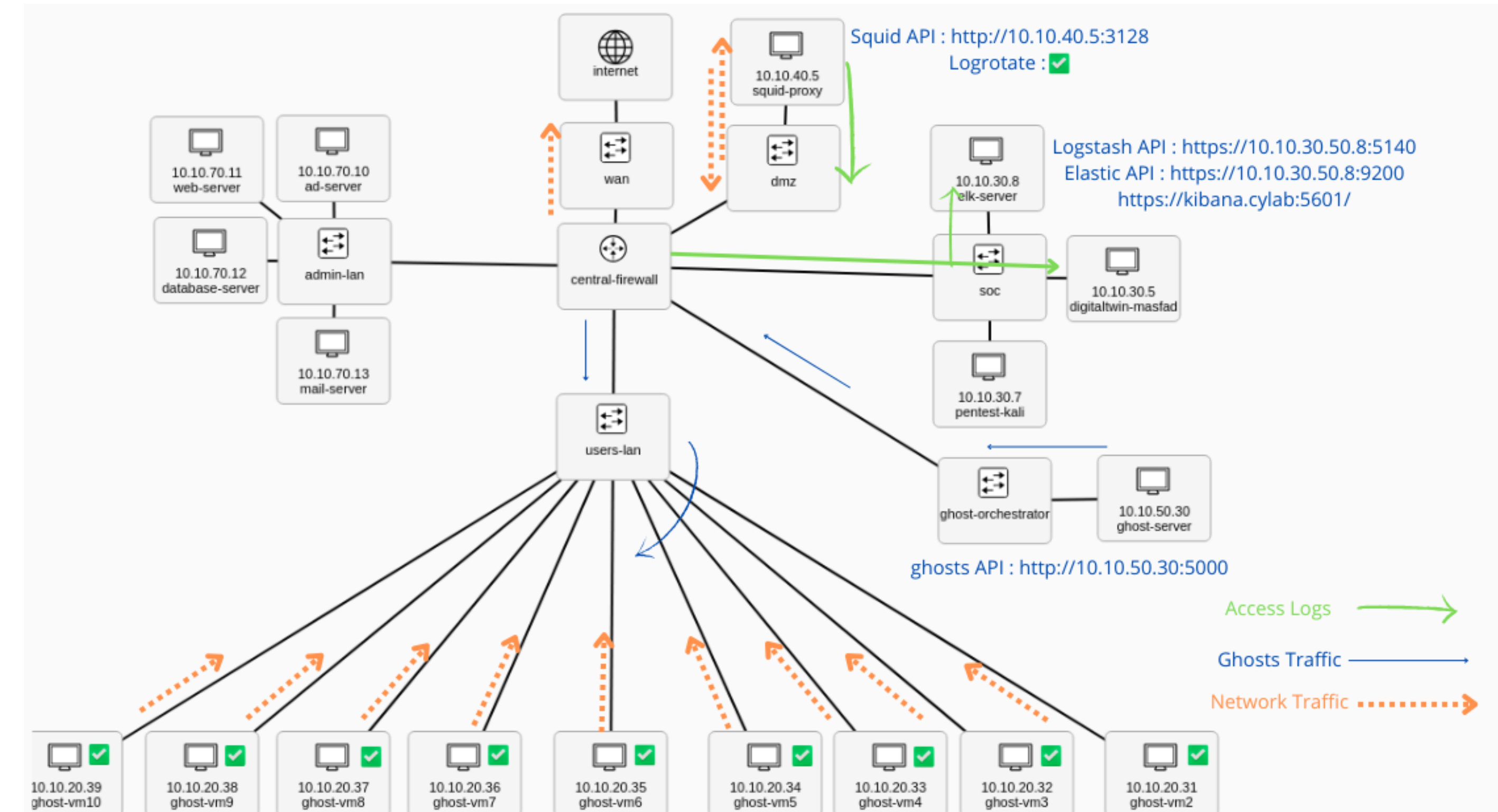
3- Target of Evaluation: MASFAD

TOE boundary: MASFAD is the Target of Evaluation; the Digital Twin represents its operational environment, not the TOE itself.

Evaluation role: the DT provides controlled deployment context, telemetry sources, benign workload, and adversarial stimuli.

Assessment focus: MASFAD is evaluated through observable behavior under declared operational assumptions.

4- Digital Twin Architecture



The DT reproduces an enterprise-style environment with segmented networks, controlled egress, centralized telemetry, benign workloads, and MASFAD deployment.

Segmentation: user, administration, DMZ, SOC, orchestration, and attacker networks.

Controlled egress: Squid centralizes outbound traffic.

Telemetry: ELK centralizes proxy, service, endpoint, and detection events.

Parallel deployment: the same sandbox can be instantiated multiple times within a KYPO pool.

Isolation: each instance preserves its topology, services, scenarios, telemetry, and evidence.

5- Evaluation Scope

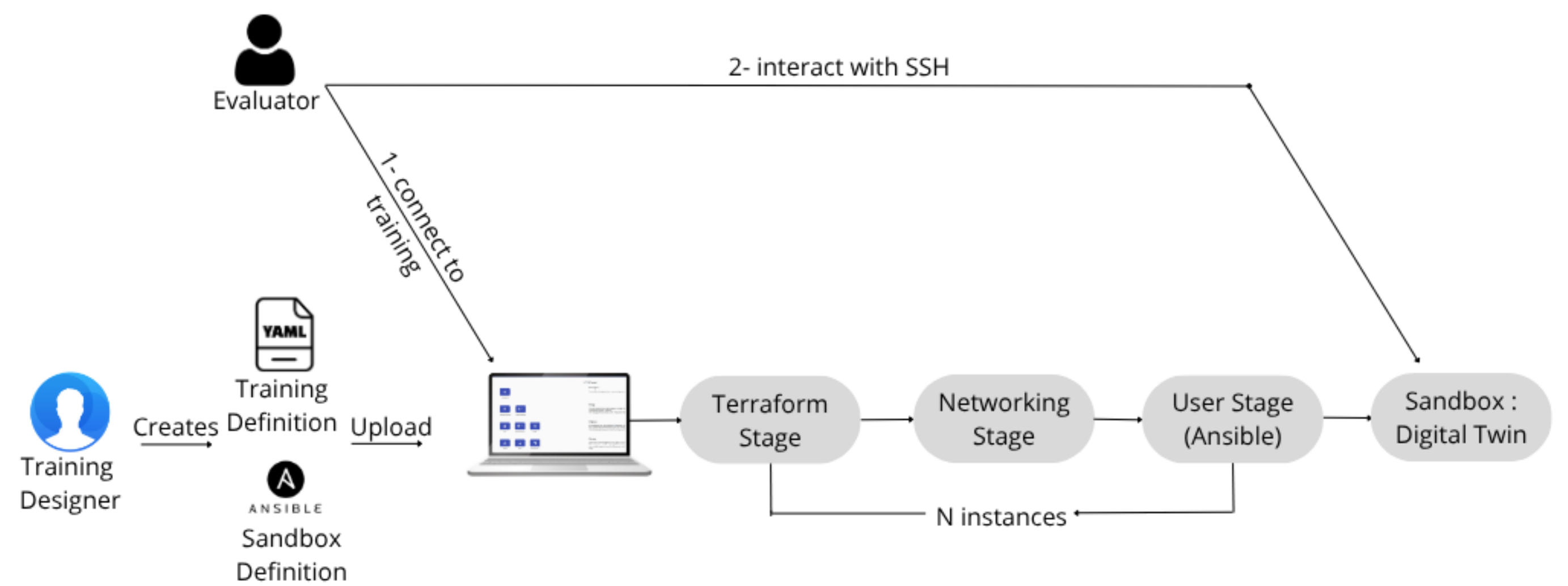
TOE under test: MASFAD is evaluated in its operational context, including exposure, telemetry, and dependencies.

Controlled environment: the Digital Twin manages topology, services, traffic, telemetry, and scenarios.

Evidence scope: evidence covers proxy logs, endpoint artifacts, service activity, and MASFAD outputs.

Certification support: the environment enables repeatable TOE observation without replacing formal Common Criteria evaluation.

6- Deployment Workflow



Input: a KYPO sandbox definition describes the topology, networks, hosts, and deployment constraints.

Infrastructure instantiation: Terraform creates the virtual resources, networks, and connectivity required by the DT.

Host provisioning: Ansible configures services, endpoints, telemetry sources, GHOSTS components, and MASFAD.

Output: an executable and repeatable Digital Twin instance ready for benign workload generation, adversarial scenario execution, and evidence collection.

7- Traffic Generation

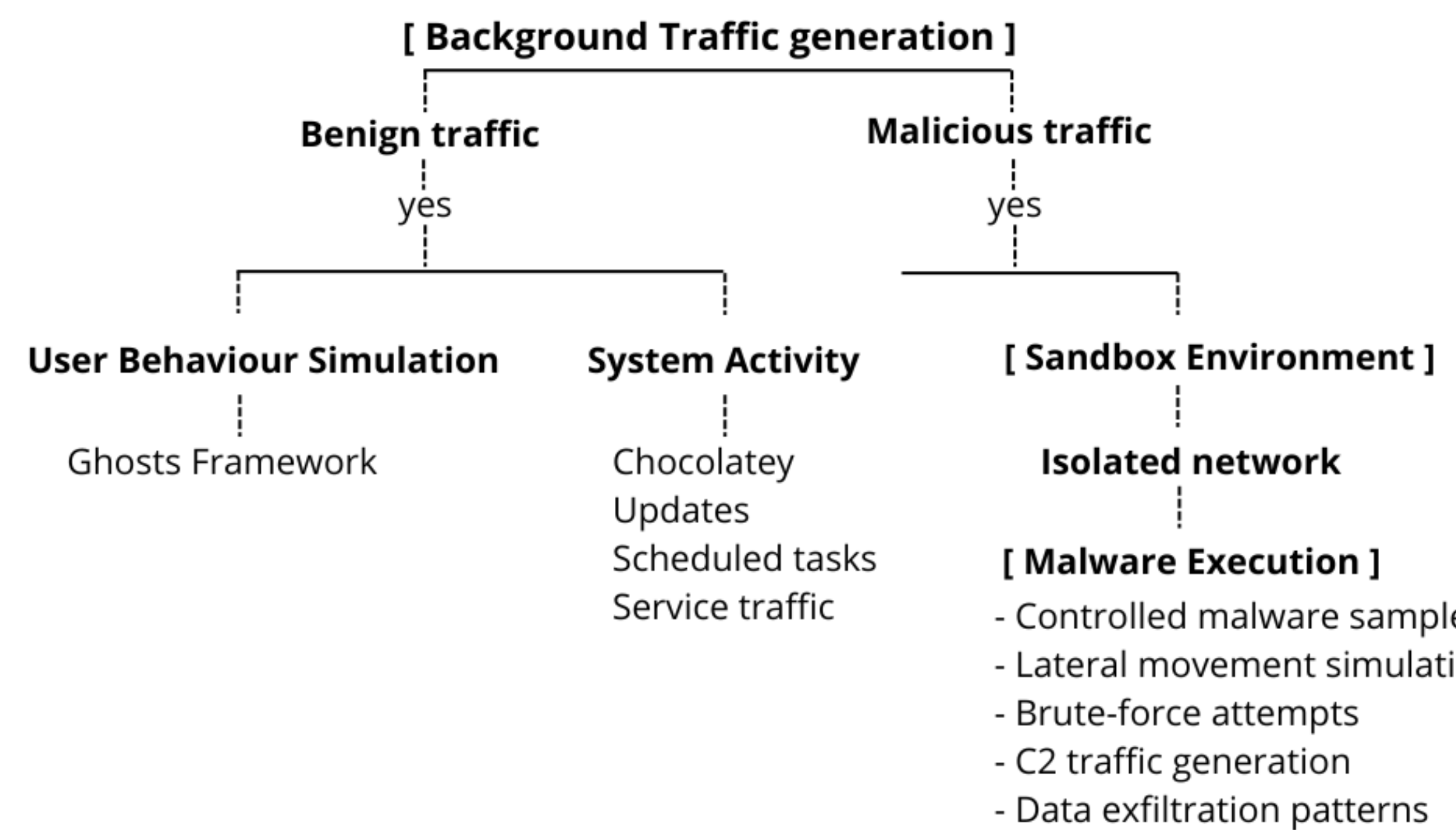
Controlled workload: combines GHOSTS-based [4] user behavior, routine activity, and isolated adversarial scenarios.

Benign activity: generates realistic web, service, installation, scheduled-task, and update traffic.

Malicious activity: executes repeatable scenarios producing attack-related flows and host artifacts.

Telemetry collection: captures proxy, endpoint, service, and detection-level events.

Evaluation use: provides time-correlated evidence for inspection, replay, and cross-deployment comparison.



8- Validation Results & Certification Relevance

Validation assessed reproducibility, workload execution, telemetry observability, and evidence generation.

Reproducibility: 5 redeployments confirmed stable topology, telemetry, and MASFAD integration.

Workload execution: validation covered 72 hours of benign activity and 4 controlled adversarial scenarios.

Telemetry observability: ELK indexed 196,549 Squid records, confirming controlled egress capture.

Evidence generation: MASFAD generated 445 evidence records from 2,592 jobs for replay-oriented analysis.

Configuration control: the same DT definition supports repeated evaluation runs under explicit assumptions.

CC-oriented support: the DT supports ATE and AVA activities while preserving deployment and telemetry assumptions.

9- Conclusion and Future Work

Conclusion: the KYPO-based DT provides a repeatable and traceable environment for certification-oriented evaluation of MASFAD while preserving the boundary between the TOE and its supporting infrastructure.

Future work: extend the proof-of-concept with stronger Common Criteria activity mapping, a larger ATT&CK-inspired scenario catalog, additional redeployment experiments, and explicit criteria for reproducibility, telemetry completeness, and operational representativeness.

References

- [1] AMC3 Project, *Automated Methods for Cybersecurity Certification of defense Software*, Belgian defence-related Research Action.
- [2] MASFAD, *Multi-Agent System for APT Detection*, Royal Military Academy, Cyber defense Lab.
- [3] KYPO Cyber Range, *Cyber Range Platform*.
- [4] Carnegie Mellon University Software Engineering Institute, *GHOSTS: General Human-Oriented Synthetic Teammates and Systems*, software repository.

