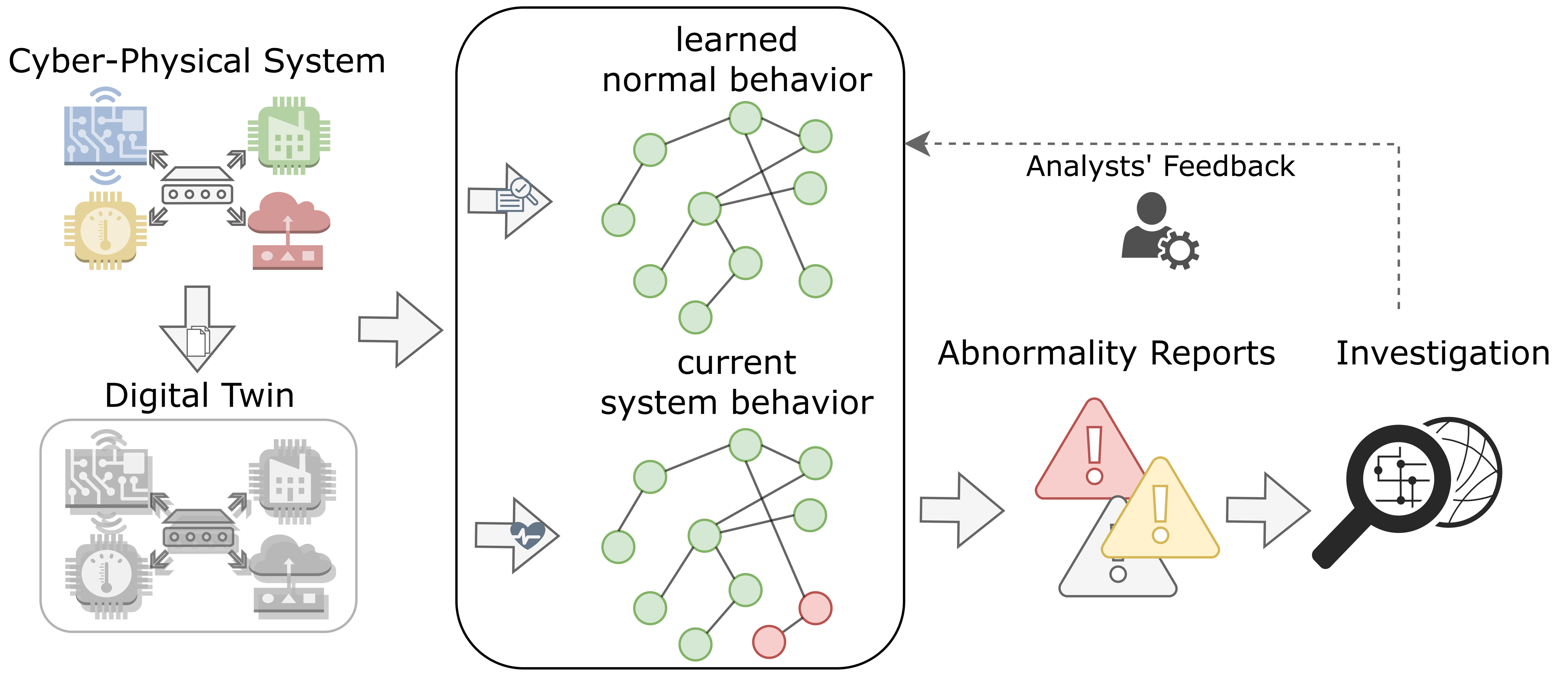
A Novel Threat Hunting Approach for APT Activities based on Anomaly Detection

Robin Buchta, Carsten Kleiner, Felix Heine, Daniel Mahrenholz, Uwe Mönks, Henning Trsek

Concept for Semi-Automated Threat Hunting



Motivation & Objective

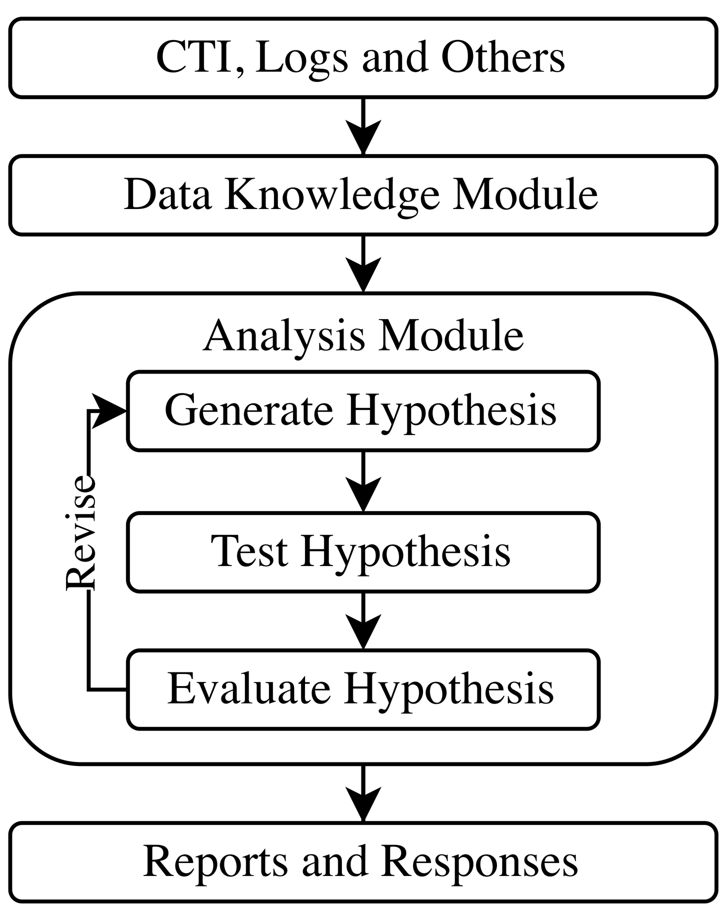
Cyber-physical systems (CPS) have become integral to critical infrastructure, making their security an important concern. Established security measures often fall short in defending against sophisticated threats such as advanced persistent threats (APT), characterized by their stealth and persistence [1].
Our framework, GraphWatch, tackles the challenge of threat hunting in CPS. Specifically, it operates as follows: given an instantiation (g), it takes a hypothesis (h), utilizes graph-based anomaly detection (f), and returns an answer (a) along with a set of new hypotheses (H).

Preliminary Results and Discussion

- Features of GraphWatch:
  - New Threat Hunting Variant: Introduces a new category, Graph-ML, combining graph methods with machine learning.
  - Automated Hypothesis: Uses system activity deviation scores for hypothesis generation, enriched with context and CTI, focusing on insider threats.
  - Data Representation: Graphs for anomaly detection and manual investigation.
  - Data Quality: Evaluates important data sources, transforms data into a heterogeneous graph structure, and handles continuous and current system status data.
  - One-Class Learning: Unsupervised GNN-based anomaly detection, using temporal heterogeneous multi-graphs.
- Challenges:
  - Requires normal behavior data for machine learning.
  - Dealing with changed normal behavior.

Threat Hunting

- The main task of threat hunting is an interactive process that involves human reasoning procedures, inspecting outcomes, and iteratively revising threat hypotheses based on observations and related knowledge [2, 3].
- The threat hunting cycle has four steps [2]:
  1. Hypothesis generation
  2. Investigation
  3. Evaluate results
  4. Actions/enrichment of the knowledge base
- This time-consuming and resource-intensive process makes automation highly desirable.
- With GraphWatch, we want to integrate threat hunting with anomaly detection and continuously improve the GNN through human feedback.



Simplified threat hunting system, based on [2].

Next Steps

- Collect data from SmartFactoryOWL demonstrators.
- Develop integration and detection methods and build the digital twin.
- Evaluate and adapt GraphWatch based on related APT detection work.

Conclusion

- Research Focus: Introducing a novel approach for detecting APT activities in CPS using semi-automated threat hunting and graph-based anomaly detection.
- Core Hypothesis: Attackers fail to perfectly mimic normal behavior, making them detectable through anomaly detection.
- GraphWatch: Threat Hunting based on Graphs
  - GraphWatch uses graphs to model system entity relationships and behaviors.
  - GNN learns normal system behavior from the graph, detecting anomalies for manual investigation.

Methodology

- Approach: Experimental, using CPS demonstrators.
- Data Sources: SmartFactoryOWL [4], digital twins, and public datasets.
- Data Collection: Open-source solutions with custom solutions for proprietary protocols.
- Threat Hunting: Graph-based and focused on system behavior, anomaly detection, and Cyber Threat Intelligence (CTI)-enriched context, the targets are insider threats and APT.
- Graph Construction: Hypothesis-based subgraph generation.
- Evaluation: Anomalies tested via graph analysis, feedback loop improves detection, detection performance measured by F1 score and analyst involvement.

References

[1] Adam Khalid et al. "Advanced Persistent Threat Detection: A Survey". In: *2021 3rd International Cyber Resilience Conference (CRC)*. 2021, pp. 1–6. doi: 10.1109/CRC50527.2021.9392626.

[2] Boubakr Nour, Makan Pourzandi, and Mourad Debbabi. "A Survey on Threat Hunting in Enterprise Networks". In: *IEEE Communications Surveys & Tutorials* 25.4 (2023), pp. 2299–2324. doi: 10.1109/COMST.2023.3299519.

[3] Xiaokui Shu et al. "Threat Intelligence Computing". In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. CCS '18. Toronto, Canada: Association for Computing Machinery, 2018, pp. 1883–1898. isbn: 9781450356930. doi: 10.1145/3243734.3243829. url: https://doi.org/10.1145/3243734.3243829.

[4] *SmartFactoryOWL*. https://smartfactory-owl.de. Accessed: August 28, 2024.