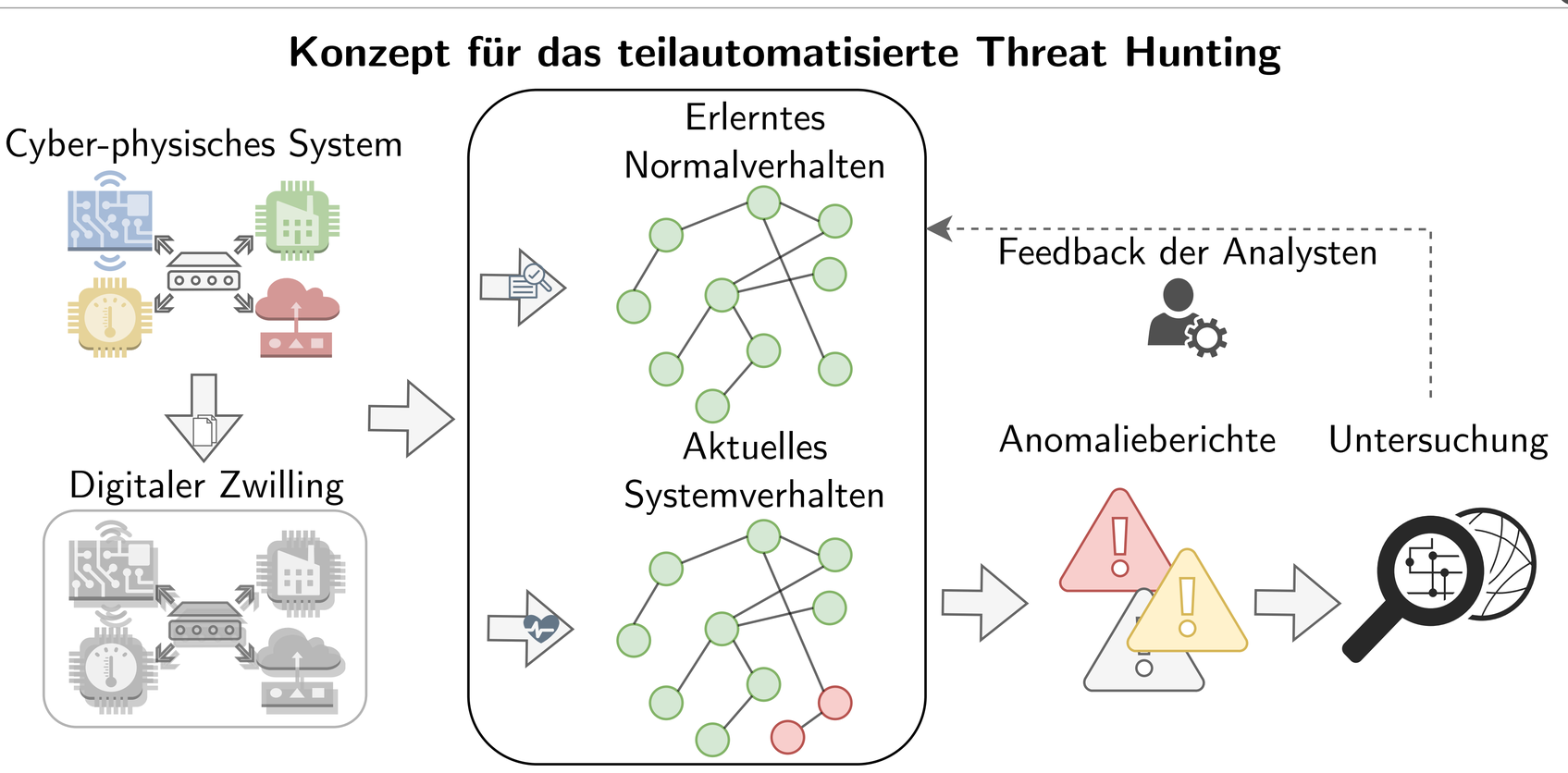
GraphWatch

Teilautomatisiertes Threat Hunting mit Graph Neural Networks für Cyber-physische Systeme



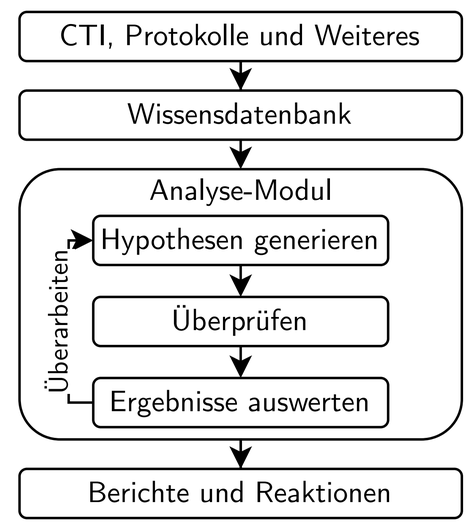
Motivation & Zielsetzung

- Cyber-physische Systeme (CPS) sind essenziell für kritische Infrastrukturen, wodurch ihre Sicherheit von besonderer Bedeutung ist.
- Etablierte Maßnahmen genügen oft nicht, um hochentwickelte Bedrohungen wie Advanced Persistent Threats (APT) zu erkennen [1].
- Das Framework GraphWatch (g) adressiert Threat Hunting in CPS:
  - Eingabe: Eine Bedrohungshypothese (h), z. B. „Insider exfiltriert Daten“.
  - Verarbeitung: Graphbasierte Anomalieerkennung (f).
  - Ausgabe: Eine Antwort (a) und neue Hypothesen (H).

$$\mathrm{a},\mathrm{H}=g\left(\mathrm{h},f\left(\right)\right)$$

Threat Hunting

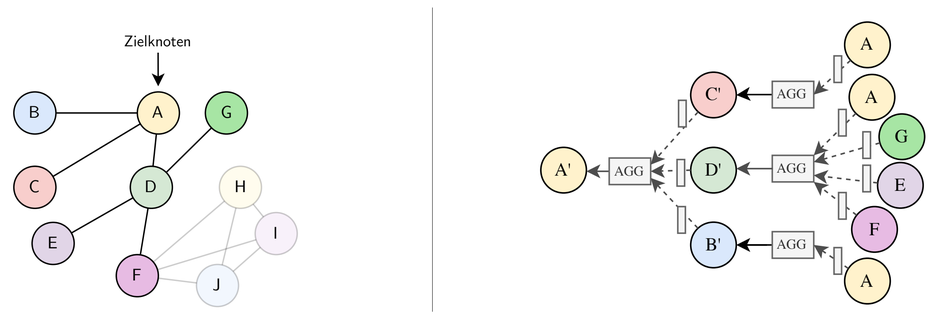
- Threat Hunting beschreibt einen interaktiven Prozess, der menschliche Schlussfolgerungen, die Überprüfung von Meldungen und die iterative Überarbeitung von Bedrohungshypothesen auf der Grundlage von Beobachtungen und damit verbundenem Wissen umfasst [3, 4].
- Die Hypothesengenerierung ist sowohl von äußeren Einflüssen als auch vom Analysten abhängig, während die Validierung hauptsächlich vom Analysten erfolgt.
- Threat Hunting ist zeit- und ressourcenintensiv. Eine Automatisierung ist daher erstrebenswert.



Threat Hunting-System, basierend auf [3].

Graph Neural Networks

- Zur Erkennung von APT-Aktivitäten nutzen wir Nachbarschaftsinformationen im Graph, um verschleierte Aktionen aufzudecken.
- Das Message Passing (MP) Framework wird auf die 2-Hop-Nachbarschaft des Zielknotens A angewendet.
- Das Ergebnis ist eine erweiterte Darstellung A′ des Zielknotens, die für die Anomalieerkennung genutzt wird. Abbildung basiert auf [2].



Vorläufige Ergebnisse

- Graph-ML als neue Variante des Threat Huntings, die Graph-Methoden mit maschinellem Lernen kombiniert.
- Verwendet Abweichungen der Systemaktivität zur automatisierten Hypothesenbildung, angereichert mit Kontext und Cyber Threat Intelligence.
- Verwendet die Darstellung der Daten als Graphen zur Anomalieerkennung und -auswertung.
- Unterstützte Hypothesenvalidierung durch die Meldung von priorisierten verdächtigen Teilgraphen.
- One-Class Learning ermöglicht die Erkennung von Angriffen, ohne Angriffe zu lernen. Möglich durch self-supervised Classification oder mittels Negative Sampling.
- GNN-basierte Anomalie-Erkennung, um Nachbarschaftsbeziehungen zu nutzen. GNN als Hilfsaufgabe zur Generierung von höherwertigen Repräsentationen der Knoten, die dann für das One-Class Learning verwendet werden.

Fazit

- Forschungsschwerpunkt: Einführung eines neuartigen Ansatzes zur Erkennung von APT-Aktivitäten in CPS unter Verwendung von teilautomatisiertem Threat Hunting und graphbasierter Anomalieerkennung.
- Forschungshypothese: Angreifer können normales Verhalten nicht perfekt imitieren, sodass sie durch Anomalieerkennung identifiziert werden.
- Aktuelle Herausforderungen:
  - Benötigt Normalverhaltensdaten für das maschinelle Lernen.
  - Umgang mit verändertem Normalverhalten.
  - Erkennung von verschleierten Aktivitäten.

Referenzen

[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] William L. Hamilton. “Graph Representation Learning”. In: *Synthesis Lectures on Artificial Intelligence and Machine Learning* 14.3 (2020), pp. 1–159. url: https://www.cs.mcgill.ca/~wlh/grl_book/files/GRL_Book.pdf.

[3] 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.

[4] 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.

Kontaktdaten

Robin Buchta, Felix Heine, Carsten Kleiner

- robin.buchta@hs-hannover.de
- felix.heine@hs-hannover.de
- carsten.kleiner@hs-hannover.de

DataIH INSTITUTE FOR APPLIED DATA SCIENCE HANNOVER

rt-solutions.de experts you can trust.

inIT | TH OWL

GEFÖRDERT VOM Bundesministerium für Bildung und Forschung