Investigating Adversarial Patterns in Linux Environments Using Weighted Knowledge Graphs

Akinyemi Anuoluwapo, Martins Jurema

November 2025

1 Introduction

Internet defense has become a task that requires analytical depth rather than rule-based reaction due to the ongoing growth of cyber threats. The complex chains of tactics used by contemporary adversaries—initial access, privilege escalation, persistence, and exfiltration—occur concurrently or recursively within enterprise systems. Understanding the connections between distinct events that together characterize purpose is more important for detecting such behavior than log correlation alone. Recent studies emphasize that threat detection systems can identify contextual relationships between acts, such as privilege escalation followed by data exfiltration, when behavioral sequences are represented in relational or graph-based structures. With this method, researchers can spot coordinated harmful activity that could otherwise seem harmless on its own. By lowering spurious correlations between unrelated security events and improving detection reliability and interpretability, the authors contend that such structured modeling makes it possible to reconstruct attacker intent more clearly. Daszczyszak, Ellis and Whitley (2019) point out that using the miter ATTCKparadigm to map adversarial behavior to tactics, techniques, and procedures (TTPs) might help us better understand it. They clarify that because traditional detection techniques concentrate too much on individual events or signs, they frequently overlook the attackers' larger operational aim. The logical progression of an infiltration campaign is revealed by TTP-based hunting, which compares observed behaviors with known adversarial patterns. Using this structured mapping, analysts can better predict the moves of attackers, combine disparate signs into cohesive stories, and support proactive threat-hunting and forensic reconstruction initiatives. [1][2]. the usefulness of graph-based models in understanding hostile conduct. According to their data, some MITRE ATTCK tactics frequently occur together in the same intrusion campaigns, indicating regular behavioral dependencies as opposed to chance events. Visualization of these co-occurrences as a graph reveals that certain techniques—in particular, the Command and Scripting Interpreter (T1059) and 2 Ingress Tool Transfer (T1105)—are the "main "hubs" that link several attack paths. These techniques often interact with other techniques across campaigns.

The authors point out that, in order to remain persistent and situationally aware, adversaries also frequently employ Defense Evasion (TA0005) and Discovery (TA0007) strategies, frequently combining them with other actions. A clearer and easier-to-understand picture of how assaults develop is provided by graph-based visualization because to this relational mapping, which enables analysts to spot patterns that conventional statistical techniques frequently overlook. When combined with the MITRE ATTCKframework, graph-based analysis provides a standardized semantic structure that allows diverse telemetry sources to be meaningfully aligned and compared. As noted by Chamkar, Maleh, and Gherabi (2024), the ATTCKframework "serves as a critical tool to improve threat intelligence, security monitoring, and incident response," helping analysts systematically map adversarial behaviors and prioritize defensive measures. Furthermore, aligning network or system data with ATTCK matrices enables quantitative visibility into detection coverage, allowing organizations to "conduct gap analyses for assessment and improvement." The Cybersecurity and Infrastructure Security Agency (CISA) further emphasizes that consistent and precise mapping of attack behaviors to ATTCK techniques is central to producing coherent adversary profiles and activity trend analysis, which in turn strengthens detection and mitigation strategies. This underscores how the integration of graph models with ATTCKnot only standardizes behavioral interpretation but also transforms fragmented telemetry into an interpretable, comparative landscape for cyber threat intelligence. [3] present a versatile, graph-based method for identifying cyberthreats that creates a structured knowledge graph from raw Linux kernel audit data. Their method, known as THKG, reveals connections between files, processes, and network activity by fusing audit data with expert knowledge and threat intelligence. Despite their detail, kernel logs are frequently big, complicated, and semantically separated, which makes analysis challenging. The technique enables analysts to carry out interactive attack exploration, causal tracing, and real-time monitoring by transforming these logs into a clearly defined graph representation. The method provided a scalable and explicable framework for contemporary threat hunting and shown efficacy in identifying complex threats and reconstructing entire attack paths when tested using DARPA Transparent Computing datasets. [5] The approach we propose integrates Linux auditd logs within a centralized ELK-based collection and analysis pipeline, ensuring continuous monitoring and scalable data processing. Authentic telemetry is generated by controlled adversarial simulations and then normalized, enriched, and mapped to MITRE ATTCK procedures using Kusto Query Language (KQL) detection logic and Sigma rules. Raw audit events may be systematically correlated with identifiable adversarial activities thanks to this technique. A weighted, directed knowledge tree is created from this carefully selected information. In this model, co-occurrence links are represented by edges, which are dynamically weighted based on their frequency and temporal closeness within a specified observation window, while each node represents an ATTCK approach. Co-occurrence heat maps, detection 3 timelines, and subgraph visualizations are examples of analytical outputs that let analysts see how tactics group together and change throughout the course of an assault. This makes it easier to evaluate intricate incursion progressions quantitatively and visually. a. Empirical Verification on Diverse Platforms The graph-guided analytical model is empirically validated in this study on a variety of operating systems, including Linux and Windows. Through a comparison of co-occurrence structures obtained from several telemetry sources, the study evaluates the method's resilience and flexibility. The findings show that even when log semantics, system architecture, and event syntax vary between platforms, the model is still able to accurately represent the semantic links across approaches. b. Reproducible Telemetry-to-ATTCK Mapping Framework The creation of a replicable system that standardizes the mapping of Linux audited telemetry to ATTCKprocedures is one of this work's main contributions. This framework makes use of open-source query languages (KQL) and rule formats (Sigma) to provide interoperability, scalability, and transparency. Security teams can duplicate, modify, and expand the model for their unique contexts without relying on a vendor because to this reproducibility, which encourages cross-institutional consistency. c. Visualization Artifacts to Improve the Interpretability of Analysts The creation of visualization artifacts that convert intricate telemetry relationships into understandable graphical representations constitutes the third contribution. Investigators can gain more understandable forensic insights and a better situational awareness by using tools like temporal heatmaps, causal subgraphs, and co-occurrence matrices. The methodology enables analysts to effectively convey discoveries within multi-platform cyberdefense operations, uncover hidden links, and track attacker intent by converting dense event data into interpretable structures.

[1] M. Almukaynizi, S. Marchal, and N. Asokan, "Behavioral Modeling for Advanced Threat Detection," Computers Security, vol. 124, pp. 103078, 2023. [2] R. Daszczyszak, D. Ellis, and S. Whitley, "TTP-Based Hunting: Mapping Adversarial Behavior Using MITRE ATTCK," MITRE Tech. Rep., 2019. [3] C. Mzoughi and H. Jamal, "What Hinders Adoption of Artificial Intelligence for Cybersecurity in the Banking Sector," MDPI Information, vol. 15, no. 12, p. 760, 2024. [4] Samir Achraf Chamkar, Yassine Maleh, and Noreddine Gherabi "Security Operations Centers: Use Case Best Practices, Coverage and Gap Analysis Based on MITRE Adversarial Tactics, Techniques, and Common Knowledge," priv. 2024 [5] H. Wu, Y. Yang, and R. Li, "A Flexible Approach for Cyber Threat Hunting Based on Kernel Audit Logs," Cybersecurity, vol. 5, no. 1, pp. 1–12, 2022.