A MITRE ATT&CK-Based Anomaly Detection System Using Privacy-Preserving Security Data[*]

Hongil Ju, Jongsik Moon and Dongho Kang[†]
System Security Research Section, ETRI, Republic of Korea
{juhong, jsmoon, dhkang} @etri.re.kr

Abstract

Existing security monitoring technologies rely heavily on Cyber Threat Intelligence (CTI)-based event analysis, thus limiting the ability to accurately assess attack success or the extent of damage within internal systems. In addition, Endpoint Detection and Response (EDR)-based information collection is restricted in national critical security facilities due to privacy and security concerns. To address these limitations, this study presents an anomaly detection system based on privacy-preserving internal security information.

1. Introduction

Current security monitoring technologies primarily rely on collecting and analyzing security events detected by security solutions based on Cyber Threat Intelligence (CTI). However, this dependence makes it challenging to accurately assess the overall impact of cyber threats—including attack success, damage extent, and scope—on compromised systems and networks within an organization. Consequently, such an approach faces limitations in providing sufficient information for accurate and timely incident response. Although Endpoint Detection and Response (EDR) technology can collect internal information by installing agents on internal systems, its deployment is severely restricted in national critical security facilities due to significant privacy and security concerns.

Therefore, there is a critical need to develop security monitoring technologies that establish privacy-preserving security information capable of addressing the privacy and security issues associated with internal systems and networks. Accordingly, this paper proposes a system for asset identification and event information collection to construct an internal anomaly detection framework and implement a MITRE ATT&CK-based workflow.

2. MITRE ATT&CK-Based Anomaly Detection System

This study proposes a system for detecting host-level anomalies based on the MITRE ATT&CK framework. The proposed system utilizes an open-source agent, such as OSQuery, to collect real-time events from each host asset. These events include external domain access history, process and file execution or modification history, upload and download logs, system vulnerability information, and user activity logs, which are stored in a central database. The collected data are cross-referenced with

[*] Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-23, December 16-18, 2025, Sapporo, Japan. © The copyright of this paper remains with the author(s).

[†] Corresponding author

public Common Vulnerabilities and Exposures (CVE) lists to identify unpatched software vulnerabilities and to quantify their associated risk levels. The evaluated risks and events are then mapped to the Technique IDs of the MITRE ATT&CK framework to detect anomalous behaviors from the kill chain perspective.

Furthermore, this study develops and applies multiple threat-hunting models—including intelligence-driven, hypothesis-driven, custom-defined, and search-based approaches—along with correlation analysis techniques that automatically identify and trace relationships among threat intelligence, security events, and internal operational data to conduct in-depth threat analysis. The proposed system is designed to comprehensively assess the actual success of cyber attacks and their damage scope within an institution from the perspective of the Cyber Defense Matrix, thereby enhancing operator-centric detection and response capabilities.

Conclusion

The technology for preserving the privacy of security data can strengthen data protection capabilities by organically integrating data anonymization with security monitoring, thereby preventing the use of unnecessary sensitive information when responding to cybersecurity threats. Furthermore, security monitoring technology based on the Cyber Defense Matrix—which is composed of asset types, threat response stages, and kill chain phases—enables accurate detection and rapid response to cyber threats. It also facilitates the detection of unknown cyber threats through the automatic analysis of anomalous user and object behaviors. Through this approach, the application of cybersecurity operation technology that links internal assets with privacy-preserving internal security information is expected to play a pioneering role in relevant markets and industries.

Acknowlegement

This work was supported by the Institute of Information & Communications Technology Planning&Evaluation(IITP) grant funded by the Korea government(MSIT) (No. RS-2024-00437337, Development of technology for linking and utilizing security information and event management with privacy-preserving internal security data)

References

[1] The MITRE Corporation. *Finding Cyber Threats with ATT&CK-Based Analytics.* Technical report, MITRE Corporation, 2017.

[2] Haas, S., Sommer, R., & Fischer, M. “zeek-osquery: Host-Network Correlation for Advanced Monitoring and Intrusion Detection.” *arXiv preprint arXiv:2002.04547*, 2020.