멀티 클라우드 환경에서의 MITRE ATT&CK 기반 보안 로그 분석 시스템

손우영[1], 김세훈[1], 홍찬희[1], 김홍현[1], 최상훈[2*], 박기웅[2]
[1]세종대학교 정보보호학과 학부생
[2]세종대학교 정보보호학과 교수 (*연구교수)
wooyoung@pel.sejong.ac.kr, sehoon518@gmail.com, ghdcksgml220@gmail.com,
khh010203@gmail.com, csh0052@gmail.com, woongbak@sejong.ac.kr

A MITRE ATT&CK-Based Security Log Analysis System for Multi-Cloud Environments

Wooyoung Son[1], Sehoon Kim[1], Chanhee Hong[1], Honghyeon Kim[1],
Sang-Hoon Choi[2], Ki-Woong Park[2]
[1]Dept. of Information Security, Sejong University
[2]Dept. of Computer and Information Security, Sejong University

요 약

최근 다수의 기업과 국가기관은 서비스의 확장성 및 운용 효율성을 높이기 위해 클라우드 기술 도입을 활발히 추진하고 있다. 하지만, 기술의 빠른 확산에 비해 보안 대응은 미흡한 실정이며, 이를 보완하기 위해 다양한 클라우드 로그 분석 시스템이 제안되고 있다. 하지만, 기존 시스템의 경우, 멀티 클라우드 환경을 충분히 지원하지 않거나, 공격자 행위 분석 기준이 명확하지 않다는 한계점이 존재한다. 이에 본 논문에서는 AWS, Azure 및 GCP에서 API 또는 파일 기반으로 수집되는 다양한 보안 로그들을 STIX를 활용하여 정규화하고, STIX로 정형화된 로그로부터 사용자 및 시스템의 행위를 추출한 후, 이를 MITRE ATT&CK 프레임워크의 TTP와 매핑함으로써 잠재적인 보안위협을 식별하는 시스템을 제안한다.

1. 서론

최근 기업 및 정부기관에서는 서비스의 확장성 및 운용 효율성을 위해 클라우드 기술을 적극 도입하고 있다. 이는 멀티 클라우드 환경의 활용을 빠르게 확산하였으나, 빠르게 발전하고 있는 기술에 비해 멀티 클라우드 환경에 대한 보안위협 대응 기술은 미비한 실정이다. 하지만, 현재 상용화 혹은 연구/개발되고 있는 클라우드 보안 분석 시스템은 대부분 단일 클라우드 서비스에 특화되어 있음에 따라 멀티 클라우드 환경에서 수집되는 다양한 형태의 보안 로그를 통합하여 수집 및 분석하지 못한다는 한계점이 존재한다. 이와 더불어 현재 보안 분석은 여전히 시그니처 탐지 및 사전에 정의된 룰셋을 기반으로 수행된다는 한계가 있다.

이에, 본 논문에서는 멀티 클라우드 환경에서 수집되는 다양한 형태의 보안 로그들을 STIX를 기반으로 정규화하고, 해당 로그 내 행위 기반 데이터를 기반으로 MITRE ATT&CK 프레임워크의 TTP(Tactics, Techniques and Procedures)와 매핑함으로써 향후 발생할 수 있는 보안 위협을 식별하는 시스템을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 선행 연구된 클라우드 로그 분석 시스템에 대해 분석하며, 3장에서는 본 논문에서 제안하는 시스템에 대하여 주요 프레임워크와 함께 설명한다. 4장에서는 본 논문의 결론을 맺는다.

2. 클라우드 로그 분석 시스템

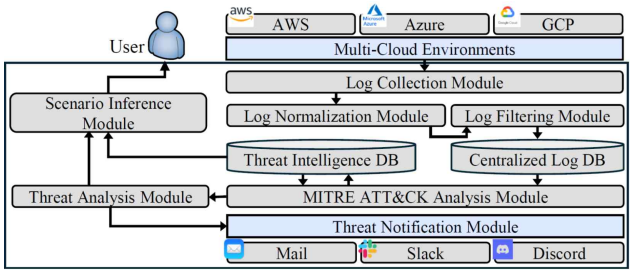
클라우드 로그 분석 시스템이란, 클라우드 환경에서 생성되는 다양한 로그 데이터를 수집, 저장 및 분석하여 시스템 성능 모니터링, 보안 위협 탐지 등을 지원하는 도구를 말한다 [1]. 클라우드 기술의 발전에 따라, 이에 대한 보안을 수행하기 위한 클라우드 로그 분석 시스템에 대한 연구가 활발히 진행되고 있다.

Y. Heo et al. [2]은 클라우드 환경의 시계열 로그 데이터를 모니터링하고 이상행위를 탐지하기 위해 트랜스포머 구조와 칼만 필터를 결합한 TKAD 시스템을 제안하였다. A. Vervaet [3]은 대규모 클라우드 환경에 적합한 자동 로그 이상 탐지 프레임워크 MoniLog를, K. Torkura et al. [4]은 멀티 클라우드 인프라의 지속 모니터링을 통해 공격자의 악성 활동과 미승인 변경을 탐지하는 CSBAuditor를 제안하였다.

기존 시스템들은 멀티 클라우드 환경을 지원하지 않거나, 공격자 행위 분석 기준이 불명확하다는 한계점이 존재한다. 이를 극복하기 위해, 공격자의 행위를 체계적으로 분석할 수 있는 모델이 요구되며, MITRE ATT&CK 프레임워크는 이러한 요구를 충족하는 Tactic-Technique 기반 위협 모델링 체계이다. 그러나, 현재까지 연구/개발된 멀티 클라우드 보안 모니터링 시스템 중, 이를 효과적으로 적용한 시스템이 부재한 상황이다.

<표 1> 클라우드 로그 분석 시스템의 주요 기능 분석

Ref	멀티 클라우드 환경 지원	로그 정규화 수행	TTP 기반 매칭	TTP 기반 공격 시나리오 예측
Y. Heo et al. [2]	X	X	X	X
A. Vervaet [3]	O	O	X	X
K. Torkura et al. [4]	O	O	X	X
Proposed System	O	O	O	O



(그림 1) 제안하는 클라우드 로그 분석 시스템

3. 제안하는 시스템

단일 클라우드 로그 분석 시스템에 집중하고 있는 한계를 보완하기 위해 본 장에서는 멀티 클라우드 환경에서 로그를 수집 및 정규화하여 MITRE ATT&CK 프레임워크를 기반으로 분석함으로써 발생 가능한 보안위협을 예측하여 식별하는 시스템을 제안한다.

먼저, 제안하는 시스템은 AWS, Azure, GCP로 구성된 멀티 클라우드 환경에서 수집되는 다양한 형태의 보안 로그를 통합 분석하기 위한 구조를 가진다. 각 환경의 원시 로그는 Log Collection Module을 통해 수집된 후, Log Normalization Module에서 STIX 기반의 표준 형식으로 정규화함으로써 로그 형식의 이질성을 제거하고 분석 효율성을 높인다. STIX 기반의 정규화된 로그는 TAXII 프로토콜을 기반으로 전달되어 Log Filtering Module을 통해 보안 관련 이벤트만을 선별한 뒤 Centralized Log DB에 저장된다. 이후, MITRE ATT&CK Analysis Module이 저장된 로그를 분석하여 해당 이벤트가 어떤 TTP와 관련되는지를 식별하고 매핑한다. 이러한 TTP 매핑 과정을 통해 개별 로그 이벤트가 공격자의 Tactic 및 Technique과 어떻게 연결되는지를 명확히 파악할 수 있으며, 이는 단순 이벤트 나열이 아닌 공격자의 의도를 구조적으로 해석할 수 있게 한다. 제안하는 시스템에서의 이러한 행위 기반 TTP 매핑은 이후 공격 시나리오를 구성하는 데 핵심적인 정보를 제공한다.

로그에 대한 TTP 매핑 결과는 Threat Analysis Module로 전달되어 위협 점수가 산정되며, 임계값을 초과할 경우 Threat Notification Module을 통해 관리자 및 사용자에게 알림이 전송된다. 마지막으로, Scenario Interface Module은 TTP 매핑 결과를 시간 순서에 따라 정렬하고, 이를 기반으로 MITRE ATT&CK의 전술 간 관계를 활용하여 과거 및 현재까지의 공격 흐름을 시나리오로 재구성한다.

이때, 제안하는 시스템의 경우, 단순히 과거 및 현재의 공격 기법을 분석하는 데 그치지 않고, 현재까지 탐지된 공격 경로를 기반으로 향후 전개 가능성이 높은 공격 기법과 전술을 예측하는 기능을 함께 수행한다. 예를 들어, T1078.004(Valid Accounts: Cloud Accounts)와 T1526(Cloud Service Discovery)가 탐지된 경우, 공격자는 이후, 내부 자산 탐색 후 T1098.003(Account Manipulation: Additional Cloud Roles)을 통해 권한을 확장하거나, T1537(Transfer Data to Cloud Account) 기법을 통해 민감 데이터를 외부 클라우드 계정으로 유출할 가능성이 높음을 예측할 수 있다. 이러한 예측은 Threat Intelligence DB에 저장된 전술 간 전이 가능성, 기법 간 연관성, 과거 유사 시나리오 사례 등을 기반으로 수행된다. 이에 따라 제안하는 시스템의 경우, MITRE ATT&CK 프레임워크를 사후 분석이 아닌 예측을 통한 선제적 대응 수단에 활용되었다는 것에 의의를 가지며, <표 1>을 통해 확인할 수 있듯이 기존 연구/개발된 도구와 비교하여 TTP 기반 매칭을 활용한 TTP 기반 공격 시나리오 예측 및 대응을 통해 능동적인 보안 운영이 가능하다는 장점이 있다.

4. 결론

본 논문에서는 기존 클라우드 로그 분석 시스템의 한계점을 완화하기 위하여 멀티 클라우드 환경에서 수집된 다양한 형태의 로그들을 구조화하고, MITRE ATT&CK의 TTP와 매핑하여 발생 가능한 공격을 제시하는 시스템을 제안하였다. 향후 연구에서는 제안된 시스템을 기반으로, 보안 분석 결과를 사용자 및 관리자가 직관적으로 활용할 수 있도록 멀티 클라우드 환경에 최적화된 커스터마이징 대시보드 설계를 목표로 한다.

Acknowledgement

한국연구재단(NRF) 중견후속연구사업(Project No. RS-2023-00208460, 100%)의 지원을 받아 수행된 연구임.

참고문헌

[1] "Cloud Log Analytics", [Online]. Available: https://www.ncloud.com/product/management/cloudLogAnalytics [Accessed: Apr. 3, 2025].

[2] Y. Heo and H. Yu, "TKAD: Transformer Networks and Kalman Filter-based Approach for Anomaly Detection in cloud System Time-Series Logs", in *Proc. ACK 2024*, vol. 31, no. 2, pp. 580-583, Oct. 2024.

[3] A. Vervaet, "MoniLog: An Automated Log-Based Anomaly Detection System for Cloud Computing Infrastructures", in *Proc. IEEE 37th Int. Conf. on Data Engineering*, Oct. 2023.

[4] K. Torkura et al., "Continuous Auditing & Threat Detection in Multi-Cloud Infrastructure", *Elsevier*, vol. 102, Mar. 2021.