보안성 관점에서의 단일/멀티 클라우드 서비스 설계 동향

김예찬, 김예진, 안승민, 권다은, 김동찬*
국민대학교

{tomking0820, alice1225kim, bryan0126, ekdms3809, dckim*}@kookmin.ac.kr

Security Considerations in Single/Multi-Cloud Service Architectures

Kim Yae-Chan, Kim Ye-Jin, Ahn Seung-Min, Kwon Da-Eun, Kim Dong-Chan*
Kookmin Univ.

요 약

본 논문은 클라우드 보안 연구 동향을 단일 클라우드(AWS)와 멀티 클라우드 환경으로 구분하여, 관리 로그와 경보가 행위 단위 및 사건 흐름 단위로 재구성되는 해석 접근을 비교·분석한다. 단일 클라우드 범주에서는 CloudTrail 기반 이상 행위 탐지, GuardDuty 경보 기반 사고 흐름 구성, eBPF 기반 워크로드 내부 관측 결합의 세 접근을 정리하고, 관측 지점과 해석 단위가 서로 달라 관리 계층 중심 관측의 한계를 보완할 수 있음을 제시한다. 반면 멀티 클라우드 환경에서는 제공자별 권한 모델, 이벤트 표현, 경보 분류 및 심각도 체계의 불일치로 인해 환경 간 행위 비교와 운영 우선순위 판단의 일관성이 저하되는 구조적 문제를 제시한다. 이를 바탕으로 공통 체계(MITRE ATT&CK) 기반 의미 정규화, 통합 등급 체계로의 심각도 재매핑, CSP 고유 맥락 보존, 정규화·재매핑 결과의 운영 판단 연계를 포함하는 통합 해석 구조의 설계 요건(R1– R4)을 도출한다.

Ⅰ. 서 론

조직이 자체 인프라를 운영하는 온프레미스 환경에서 클라우드 환경으로의 전환은 인프라 확장성, 운영 자동화, 비용 효율성 등 구조적 이점을 활용하기 위한 흐름이다. 보안 분석의 초점도 개별 서버의 내부 상태에서 벗어나, 동적으로 변화하는 권한 구성의 변화와 관리 행위로 이동하였다. 이에 따라 클라우드 보안 연구는 관리 로그를 기반으로 행위 단위와 사건 흐름 단위로 재구성하여 분석하는 접근을 중심으로 전개되고 있다. 그러나 하나의 조직이 두 개 이상의 클라우드 서비스 제공자(CSP)를 병행 운영하는 멀티 클라우드 환경에서는 CSP별 로그 구조와 이벤트 표현이 상이하고, 경보 분류 및 심각도 체계 또한 다르다. 따라서 단일 클라우드 환경에서의 해석 방식은 일관된 대응 우선순위 결정으로 확장되기 어렵다.

본 논문은 단일 클라우드(AWS)와 멀티 클라우드 환경으로 구분하여 비교 분석을 수행하였다. 단일 클라우드 범주에서는 관리 로그 및 경보를 행위 단위 및 사건 흐름 단위로 재구성하는 해석 접근을 중심으로 정리하였다[1,2,3]. 멀티 클라우드 범주에서는 CSP별 로그·이벤트·경보 표현과 심각도 체계의 불일치가 운영 단계의 비교 및 우선순위 판단을 어렵게 만드는 요인에 주목하고, 이를 공통 분류 체계에 맞춰 정규화 및 매핑하려는 통합 접근을 종합하였다[4,5].

논문의 구성은 다음과 같다. Ⅱ절에서는 단일 클라우드(AWS) 환경의 해석 접근을, Ⅲ절에서는 멀티 클라우드 환경의 구조적 불일치와 통합 운영 과제를 분석한다.

Ⅱ. 단일 클라우드 환경에서의 보안 관측 및 해석 접근

단일 클라우드 환경의 보안 연구들은 공통적으로 사건 흐름 단위 해석의 한계를 문제로 설정한다. 클라우드 환경에서는 권한 변경, 리소스 생성·삭제, 설정 수정 등 관리 행위가 빈번하게 발생하며, 이를 개별 로그로만 해석하려는 경우 정상 운영과 침해 상황이 서로 유사한 양상으로 관측될 수 있다. 따라서 보안 관측은 로그 간 관계와 시간적 순서를 해석하는 과정에 의존한다.

이에 따라 최근 연구들은 관측 단위를 개별 로그에서 시간적으로 연결된 행위들의 흐름으로 재정의한다. 즉 관측의 초점은 '무엇이 발생했는가'에서 '어떤 맥락에서, 어떤 연쇄를 통해 발생했는가'로 이동한다.

i. 로그 기반 이상 행위 해석 중심 접근

이상 행위 탐지 프레임워크는 CloudTrail를 단순 기록이 아닌, 보안적으로 의미 있는 속성 (행위주체·대상·행위 종류·시점)에 따라 행위 단위로 재구성한다[1]. 이를 위해 eventName(행위 종류), eventSource 및 requestParameters(대상 서비스/리소스), user Identity(행위 주체), eventTime(시점) 등 핵심 필드를 중심으로 로그를 분해하고, 필드 값의 표현을 비교 가능하도록 정규화한다. 정규화된 이벤트는 수치화 과정을 통해 행위 벡터로 표현되며, 시간 순서에 따라 배열되어 행위 시퀀스로 구성된다. 정상 운영 구간의 행위 표현 집합은 행위 기준선(baseline)을 형성한다. 이후 신규 행위는 기준선과의 코사인 거리로 이탈 정도를 정량화하며, 이를 바탕으로 이상 여부를 판단한다. 또한 정상으로 판정된 행위를 기준선 갱신에 반영함으로써, 사전에 정의된 고정 규칙에 대한 의존을 낮추고 운영 패턴 변화에 적응할 수 있는 해석 구조를 가진다.

ii. 침해상황을 흐름으로 인식하는 관점

또한, 침해 상황을 단일 경보가 아닌 행위의 인과적 흐름으로 파악한다[2]. 이 관점에서 이상 징후를 탐지하는 AWS GuardDuty의 경보(finding)는 침해 인식의 출발점일 뿐이며, 실제 판단은 경보 전후의 CloudTrail 로그를 맥락(context)으로 연결하여 인과 관계를 구성하는 방식으로 이루어진다. 이러한 접근을 구체화한 DAC(Detection and collection of logs for Analyzing Cloud security incident) 프레임워크는 GuardDuty의 경보를 기준점으로 삼아, 경보 전후의 CloudTrail 로그를 결합하여 사건 단위 행위 흐름을 구성한다[2]. 또한 구성된 행위를 MITRE ATT&CK 기반 분류 체계로 정리함으로써, 침해 상황의 흐름으로 표준화하고 이후 분석 및 대응 단계로의 연계를 지원한다.

iii. 관리 로그 한계를 보완하기 위한 워크로드 내부 관측

CloudTrail은 권한 변경이나 리소스 설정 변경 등 관리 계층 추적에는 효과적이다. 그러나 클라우드 내부의 프로세스 실행, 파일 접근, 네트워크

통신은 로그에 기록되지 않아 관측 범위의 한계가 발생한다. 공격자가 정상적인 절차로 리소스를 생성한 뒤 내부에서 악성 행위를 수행하더라도, 관리 로그만으로는 사고의 실체를 파악하기 어렵다. 이러한 관측 범위의 한계는 관리 계층과 내부 실행 계층에서 관측되는 정보의 불일치를 야기하며, 단일 로그 만으로 행위의 연속성과 맥락을 파악하기 어렵게 만든다.

이러한 한계를 보완하기위해, eBPF(extended Berkeley Packet Filter)를 기반으로 내부 행위를 선택적으로 수집하고, 이를 MITRE ATT&CK에 매핑하여 보안적 의미를 부여한다[3]. 또한 매핑 결과를 해당 체계에 대해 사전에 학습된 LLM으로 요약 및 시나리오화하여, 내부 행위의 나열을 설명 가능한 침해 상황의 흐름으로 재구성한다. 이를 통해 클라우드 내부 실행 계층에서 발생할 수 있는 악성 행위의 해석 부담을 완화하는 방향을 제시한다.

[표 1] MITRE ATT&CK 기반 위협 모델 포함 주요 기법

구분	관측 대상	해석 단위	기준 체계
이상 행위 탐지[1]	CloudTrail	행위 벡터/시퀀스	baseline
침해 흐름 구성[2]	CloudTrail+ GuardDuty	경보 기준 사고 흐름	MITRE ATT&CK
워크로드 내부관측[3]	eBPF 이벤트	실행 행위	ATT&CK+ LLM

[표 1]은 세 접근을 관측 대상, 해석 단위, 기준 체계로 비교한 것이다. 각각 [1]이 관리 계층의 이상 행위를 탐지하고, [2]가 이를 사건 흐름으로 구조화하며, [3]이 워크로드 계층에서 가시성을 보완하는 점에서 세 접근은 상호 보완적이다. 그러나 세 접근 모두 단일 클라우드(AWS)를 전제하므로, 멀티 클라우드 환경의 통합 해석으로 확장되기 어렵다는 한계가 있다.

Ⅲ. 멀티 클라우드 환경의 구조적 문제

i. 클라우드 서비스간 구조적 차이와 구성 요소 불일치

멀티 클라우드 환경에서 문제점은 동일한 보안 개념이 제공자별로 상이하다는 점이다. 예를 들어 AWS IAM, Azure RBAC, GCP IAM은 모두 권한 관리를 담당하지만, 정책 표현 방식과 상속 구조가 다르다. 이벤트 명세와 상태 변화 표현이 달라, 동일한 행위라도 클라우드별로 상이하게 기록될 수 있다. 이러한 차이로 인해 환경 간 행위 비교와 정렬이 어렵다.

이에 대한 대응으로, 벤더별 상이한 표현을 MITRE ATT&CK 기반으로 매핑하여 공통 기준으로 정렬하는 해석 구조를 제안한다[4]. 이는 행위 비교와 정렬의 기반이 된다. 이처럼 의미적 정규화는 멀티 클라우드 통합 해석의 첫 번째 요건이다.

ii. 경보 및 심각도 기준 불일치로 인한 운영상의 문제

운영 단계의 또 다른 문제는 경보 분류 및 심각도 등급 체계의 불일치이다[5]. 동일한 행위라도 한 클라우드에서는 중간 위험으로 분류되는 반면, 다른 클라우드에서는 높은 위험 또는 정보성 경보로 표시될 수 있으며, 이는 각 제공자가 위험을 정의하는 기준 자체가 상이하기 때문이다. 따라서, 경보가 의미하는 행위의 성격과 영향을 다시 해석하고 상대적 위험 수준을 추정하는 과정이 추가로 요구된다.

[5]는 이러한 문제를 완화하기 위해 CSP별 심각도 체계를 공통 등급 체계(Critical/High/Medium/Low)로 매핑하고, 이를 기반으로 대응 순서를 결정하는 방식을 제안한다. 통합 심각도 매핑은 경보가 발생한 클라우드와 무관하게, 해당 행위가 운영 관점에서 어느 수준의 대응을 요구하는지 일관되게 판단할 수 있도록 하며, 멀티 클라우드 환경에서의 운영 의사결정을 단순화하는 장치로 설명된다. 따라서 심각도 재매핑은 통합 해석의 두 번째 요건으로 정리 될 수 있다.

iii. 통합 해석 구조를 위한 설계 요건

앞선 논의를 종합하면, 통합 해석 구조 요건은 다음과 같다.

(R1) ATT&CK 등 공통 체계 기반 의미적 정규화
(R2) 통합 등급 체계로의 심각도 재매핑
(R3) CSP별 고유 맥락(리전, 서비스 특성) 보존
(R4) 정규화·재매핑 결과를 운영 우선순위 판단 및 대응 기준으로 연결

Ⅳ. 결론

본 논문은 클라우드 보안 연구를 단일 클라우드와 멀티 클라우드로 구분하여, 로그와 경보가 사건 흐름으로 해석되는 과정을 비교·분석하였다. 또한 개별 연구에서 사용된 해석 방식과 운영 쟁점을 공통 기준으로 정리하고, 통합 해석을 위한 설계 요건을 도출하였다.

단일 클라우드 환경에서는 세 가지 접근이 확인되었다[1,2,3]. 첫째, 관리 로그를 행위 단위로 재구성하고 정상 기준선 대비 이탈을 정량화하여 이상 행위를 판단하는 방법이다. 둘째, 경보를 기준점으로 전후 로그를 결합해 침해 상황의 흐름을 구성하고, 이를 MITRE ATT&CK 체계로 표준화하는 방법이다. 셋째, 관리 로그의 한계를 보완하기 위해 워크로드 내부 관측 데이터를 결합하여 사건 설명 가능성을 높이려는 방법이다.

반면 멀티 클라우드 환경에서는 제공자별 권한 구조, 이벤트 표현, 경보 심각도 기준이 상이하여 행위 비교와 우선순위 결정이 일관되게 수행되기 어렵다[4,5]. 따라서 동일 행위를 공통 기준으로 매핑하고, 심각도를 통합 등급 체계로 재매핑하는 운영 기준이 필요하다.

본 논문은 두 환경의 연구 동향을 비교하여 멀티 클라우드 통합 해석을 위한 네 가지 설계 요건(R1– R4)을 도출하였다. 종합하면, 최근 연구는 탐지량의 증가보다 관측 데이터를 사건 흐름으로 구성하고, 환경 간 표현 차이를 정렬하여 운영 판단의 일관성을 확보하는 방향으로 전개되고 있다.

한계로는 분석 대상이 국내 문헌에 집중되어 국제 동향과의 비교가 제한적이며, 제시된 요건의 실증 검증이 수행되지 않았다는 점이 있다. 향후 연구에서는 R1– R4를 반영한 프로토타입을 구현하고, AWS–Azure–GCP 테스트베드에서 대표 공격 시나리오를 재현 하여 탐지 정확도와 운영 효율성을 정량 평가할 계획이다.

ACKNOWLEDGMENT

이 논문은 2025년도 정부(과학기술정보통신부)의 재원으로 정보통신 기획평가원의 지원을 받아 수행된 연구임(No. RS-2024-00397105, KCMVP 보안 수준 3 암호모듈 제작을 위한 핵심기술 개발).

참 고 문 헌

[1] 강대현, 김주영, 김학범, 박선희, "클라우드 로그 기반 이상 행위 탐지 프레임 워크", 한국정보보호학회 동계학술대회 논문집 Vol.35, No.2, pp.729-732, 2025 년 11월.

[2] 김도연, 김수민, 조휘정, 노태영, 안관우, 이유빈, 박후린, "AWS 로그 기반 침해사고 식별 및 대응 자동화 프레임워크", 한국정보보호학회 동계학술대회 논문집 Vol.35, No.2, pp.336-338, 2025 년 11월.

[3] 김종섭, 손창민, 김진우 "클라우드 환경에서 eBPF와 LLM을 활용한 APT 탐지 프레임워크 설계", 한국정보보호학회 동계학술대회 논문집 Vol.35, No.2, pp.339-342, 2025년 11월.

[4] 지동혁, 최상훈, 박가웅, "MITRE ATT&CK 기반 주요 클라우드 벤더별 공격 표면 및 공격 벡터 비교 분석", 한국정보보호학회 동계학술대회 논문집 Vol.35, No.2, pp.1086-1089, 2025년 11월.

[5] 공나영, 김도영, 최상훈, 박가웅, "멀티 클라우드 보안 운영 효율화를 위한 통합 심각도 매핑 모델 연구", 한국정보보호학회 동계학술대회 논문집 Vol.35, No.2, pp.693-695, 2025년 11월.