클라우드 보안 취약점 사례 기반 오픈소스 도구의 예방 및 탐지 적용 연구

지동혁[1], 최상훈[2], 박기웅[3†]
[1]세종대학교 정보보호학과 석사과정
[2]세종대학교 정보보호학과 연구교수
[3]세종대학교 정보보호학과 교수
isk06270@gmail.com, csh0052@gmail.com, woongbak@sejong.ac.kr

A Study on the Application of Open-Source Tools for Prevention and Detection Based on Cloud Security Vulnerability Cases

Dong-Hyeok Ji[1], Sang-Hoon Choi[2], Ki-Woong Park[3†]
[1,2]Syscore Lab., Sejong University
[3]Dept. of Computer and Information Security, Sejong University

요 약

클라우드 도입과 마이그레이션이 활발해짐에 따라, 멀티테넌시 구조와 인프라 공유 특성으로 인해 하나의 보안 취약점이 다수 사용자에게 영향을 줄 수 있는 위험이 증가하고 있다. 그러나 기존 연구는 도구 기능 소개·분석에 치중되어 있으며, 실제 사건 기반으로 어떤 도구를 어떻게 적용해 예방·탐지 파이프라인을 구성하는지를 다룬 사례는 드물다. 본 연구는 실제 침해사고를 분석하여, 클라우드 환경에서의 예방과 탐지를 위한 도구 파이프라인을 제안한다. 또한, 침해사고 재현 및 검증을 통해 개선 방안을 도출한다.

1. 서론

클라우드 환경은 자원의 효율적인 사용과 빠른 서비스 구축을 위해, 가상화된 인프라와 서비스 구성 요소를 다수의 사용자 환경에서 공유하는 구조를 갖는다. 이로 인해 하나의 구성 오류나 보안 취약점이 다수의 테넌트에 동시에 영향을 줄 수 있으며, 특정 서비스 제공자의 설정 방식이나 기본 정책이 사고의 영향을 미친다 [1]. 특히 인프라 재활용, 공유 이미지 사용, 멀티테넌시 구조와 같은 특성은 동일한 보안 결함이 여러 환경에서 재현되기 쉬운 조건을 만든다 [2].

이러한 구조적 특성으로 인해 클라우드에서 발생하는 보안 취약점은 단순한 설정 오류를 넘어 실제 보안 사고로 이어질 가능성이 크며, 보안 위협에 대한 대응이 점점 더 중요해지고 있다. 최근 수년간 취약점이 CVE 형태로 공개되고 있으며, 이를 악용한 공격 사례도 꾸준히 보고되고 있다. 2023년 한 해 동안 공개된 신규 CVE는 28,000건 이상으로, 이 중에는 클라우드 환경에서 일어난 취약점도 있다 [3].

이처럼 취약점 정보가 공유되고 있음에도 불구하고, 기존 연구는 보안 도구 자체의 기능 소개나 기술 분석에 집중돼 있다. 실제 보안 사건을 기반으로, 오픈소스 도구를 활용해 예방 및 탐지 관점에서 구성한 파이프라인에 관한 연구는 드물다 [4].

본 연구는 이러한 공백을 보완하고자, 최근 공개된 클라우드 취약점 사례를 중심으로 사건 개요, 공격 흐름, 주요 공격 벡터를 정리한다. 또한 각 사례에 대해 예방 및 탐지 관점에서 적용 가능한 오픈소스 도구를 제시한다. 사례 선정 기준은 다음과 같다. (1) CVE가 공개되어 기술 자료 및 재현 근거가 확보된 경우, (2) 서로 다른 클라우드 사업자 환경, (3) 서로 다른 공격 벡터, (4) 오픈소스 도구만으로 실습이 가능한 사건. 이에 따라 AWS Amplify IAM 취약점(CVE-2024-28056), Azure Synapse Analytics 취약점(CVE-2022-29972), GCP OS Login 취약점(CVE-2025-2903)을 선정하였다. 클라우드 벤더별로 한 건씩 사례를 선정한 이유는, 서비스 간 우열을 비교하기보다, 서로 다른 유형과 도구 적용 범위의

† 교신저자: 박기웅 (세종대학교 정보보호학과 교수)

차이를 드러내기 위함이다.

연구 방법은 각 사례에 대해 예방 도구와 탐지 도구를 대응시키는 방식으로 진행한다. 예방 도구는 개념 중심으로, 탐지 도구는 운영 로그 및 에이전트 이벤트 중심으로 기술한다. 벤더의 패치로 인해 사고 당시와 동일한 환경을 구성하는 데에는 제약이 있으므로, 본 연구는 동일한 공격 벡터를 재현할 수 있는 유사 환경을 구성하여 실험을 진행한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 검토하고, 3장에서는 선정된 보안 사건을 서술한다. 4장에서는 사건별로 예방 및 탐지 도구를 설명하며, 5장에서는 결론과 향후 연구 방향을 제시한다.

2. 관련 연구

기존 연구들은 오픈소스 보안 도구의 기능적 특성과 기술 분석에 초점을 맞춘 사례가 대부분이다. 본 장에서는 이와 같은 연구들을 중심으로 관련 동향을 정리한다.

2.1 SIEM 평가 연구

Manzoor 외 3인은 SME 네트워크를 모사한 테스트베드를 구축하고 Wazuh, Elastic Security, SIEMonster, OSSIM 등 네 가지 오픈소스 SIEM을 동등 조건에서 평가하였다 [4]. 연구진은 오픈소스 SIEM의 비용, 접근성 장점을 강조하는 한편, 상용 솔루션 대비 대규모 운영 편의성과 일부 고급 기능에서 한계를 지적하였다.

여러 오픈소스 SIEM을 실제 환경에 구성하고 이벤트 수집 성능과 탐지 정확도 등을 비교한 연구에서는, 로그 소스 다양성과 사용자 정의 규칙의 적용 여부가 도구의 실효성에 큰 영향을 미친다고 평가하였다 [5].

2.2 시그니처 기반 네트워크 IDS 분석

Asad 외 2인은 4년간의 시그니처 업데이트를 수집하고, 동일한 악성 트래픽에 과거 규칙과 최신 규칙을 교차 적용해 탐지율 변화와 엔진 간 경보 차이를 분석하였다 [6]. 분석 결과, 과거 규칙은 최근 악성 트래픽에 대하여 미탐을 유발한 반면 최신 규칙은 탐지율과 경보 신뢰도가 유의미하게 개선되었다.

한편, 시그니처 기반 IDS의 탐지 결과가 규칙 구성 방식에 따라 달라질 수 있다는 점을 실험적으로 분석한 연구도 있다. 이 연구는 Snort와 Suricata의 규칙 업데이트 내역을 비교하고, 동일한 트래픽에 대해 생성되는 경보의 다양성을 강조하였다 [7].

2.3 클라우드 네이티브 런타임 탐지 평가

Kumar는 Kubernetes 환경에서 ATT&CK 기반의 수평 이동, 권한 상승 시나리오를 설계하고, Falco의 규칙을 통해 시스템콜 이벤트와 Kubernetes 감사 로그를 실시간 상관, 탐지하는 능력을 평가하였다 [8].

클라우드 네이티브 환경의 보안 위협에 대응하기 위한 도구들을 다룬 최근 연구에서는 Falco 외에도 Cilium Tetragon 등의 런타임 탐지 도구가 언급되었으며, 커널 수준의 행동 기반 탐지 기능이 실시간 대응에 효과적이라는 점이 제시되었다 [9].

3. 클라우드 벤더 별 침해사고 사례

본 장에서는 AWS, Azure, GCP별로 선정한 사건을 대상으로 개요, 공격흐름, 주요 공격 벡터 순으로 정리한다.

3.1 AWS Amplify IAM 역할 취약점

AWS Amplify CLI와 Studio에서 생성된 IAM 역할에 조건 없이 설정된 신뢰 정책(trust policy)을 사용하는 취약점이 발견되었다. 공격자는 자신의 토큰을 이용해 해당 역할을 임의로 탈취할 수 있었다. 공격 흐름은 개발자가 Amplify 프로젝트에서 인증 컴포넌트를 제거하면, 관련 IAM 역할의 trust policy에서 조건 항목이 사라지고 "Effect": "Allow"만 남게 된다. 이로 인해 공격자는 자신의 일반 계정에서 API를 호출해 IAM 역할을 탈취할 수 있었다. 주요 공격 벡터는 조건 블록이 제거되어 누구나 접근 가능한 상태가 된 것이다 [10].

3.2 Azure Synapse 교차 테넌트 취약점

Orca Security 팀은 Azure Synapse Analytics에서 샌드박스 격리 우회 및 교차 테넌트 간 권한 침해가 가능한 명령어 인젝션 취약점을 발견했다 [11]. 이 취약점은 Amazon Redshift용 ODBC 드라이버의 기존 취약점을 기반으로 하며, 이를 통해 원격 코드 실행(RCE) 및 타 테넌트 계정 접근이 가능했다. 공격 흐름은, 공격자가 외부 데이터 소스 연결 시 쉘 명령을 삽입하고, VM 내에서 RCE를 한 뒤 Azure 관리 API에 접근하여 자격 증명을 탈취함으로써 다른 고객 계정에 접근했다. 주요 공격 벡터는 샌드박스 격리를 우회해 OS 수준에서 탈출한 부분이다.

3.3 GCP OS Login 기능이 활성화된 인스턴스 취약점

GCP 환경의 OS Login 기능이 활성화된 VM 인스턴스에서 권한 설정 오류로 인해 인증 우회 및 RCE가 가능한 취약점이 발견되었다 [12]. 공격자는 IAM

권한을 획득하거나 취약한 권한 구성을 악용해 특정 사용자 또는 서비스 계정으로 VM 인스턴스를 생성하고, 자신의 SSH 키를 등록해 인증 없이 로그인할 수 있었다. 이 과정에서 OS Login 기능이 SSH 공개키를 자동으로 VM에 배포하는 점을 악용했다. 결과적으로 공격자는 VM 내부에서 RCE를 수행하고, 데이터 탈취 및 시스템 손상으로 이어질 수 있었다. 주요 공격 벡터는 IAM 권한 기반 계정 자동 생성과 SSH 키 자동 등록 방식이다.

4. 클라우드 침해사고 별 예방, 탐지 도구

본 장에서는 세 가지 클라우드 보안사건 AWS Amplify IAM, Azure Synapse , GCP OS Login을 대상으로, 사건마다 예방, 탐지 도구를 각각 매핑하여 개발 목적과 주요 특징의 순서로 정리한다.

4.1 Open Policy Agnet + Conftest

OPA+Conftest는 배포 전 단계에서 코드로 적어 둔 보안 규칙으로 IaC 설정을 자동 점검해, 외부 로그인 토큰으로 역할 권한을 빌리는 기능을 쓸 때 필수 조건 등 잘못된 설정을 초기에 차단한다 [13]. 또한 배포 전과 후의 보안 규칙을 자동으로 확인한다.

4.2 Parliament

Parliament는 이미 배포된 AWS IAM 정책을 다시 점검해, 권한 남용 가능성이 있는 부분을 초기에 식별한다. 취약한 조건 등을 자동 진단하고, 심각도 제공으로 운영 점검과 감사 보고에 바로 활용이 가능하다 [14].

다음은 AWS 계정에서 테스트 역할 parl-bad-role에 s3:*, iam:PassRole, ec2:RunInstances/ec2:CreateTags 각각에 대해 Resource “*” 즉 전역 리소스로 정책을 부여하였다. 그림 1은 Parliament 정적 분석 결과, parl-bad-role에서 3건의 문제점이 발견되었다는 점을 의미한다.

(그림 1) Parliamnet 탐지 결과

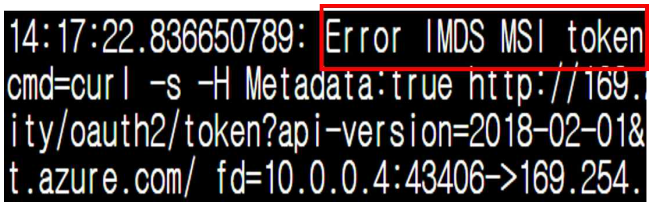
4.3 Checkov

Checkov는 Terraform/ARM/Bicep 등 IaC 정적 분석을 통해 공개 노출, 네트워크 경계를 배포 전에 차단한다 [15]. Azure를 포함한 내장 규칙, SARIF 리포트 등 파이프라인 연계를 지원하며, 규칙별 수정 가이드가 있어 재발을 예방한다.

4.4 Falco

Falco는 호스트, 컨테이너, 쿠버네티스 및 클라우드 환경 전반에 비정상 동작 및 보안 위협을 실시간으로 감지하고 경고하도록 설계되었다 [16]. Falco는 기본적으로 이벤트를 관찰하고 사용자 지정 규칙에 따라 실시간 알림을 제공하는 모니터링 및 탐지 에이전트이다.

MSI는 Azure로부터 발급되는 토큰이다. 공격자가 MSI 토큰 호출에 성공하면 엑세스 토큰을 탈취하여, 권한상승 등이 이루어 질 수 있다. 그림 2는 Falco를 실행 중인 상태에서 MSI 토큰 엔드포인트를 호출 했을 때 나오는 경고 로그이다.



(그림 2) Falco 탐지 결과

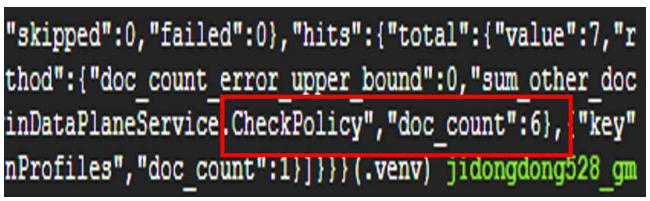
4.5 KICS

KICS는 Terraform/Kubernetes 등 IaC 정적 분석으로, OS Login 관련 잘못된 설정과 과도한 GCP IAM 바인딩을 배포 전에 차단한다 [17].

4.6 OpenSearch

OpenSearch는 GCP 감사 로그를 중앙 수집, 대시보드, 경보를 통해 비정상 로그인과 권한 변경을 탐지한다. 대규모 로그에 대한 예약 쿼리, 경보로 모니터링이 가능하며, opensearch-cli를 통해 질의와 배치 점검을 자동화할 수 있다 [18].

실험 환경에서 GCP OS Login이 활성화된 VM에 대해 SSH 접속을 시도하면, 데이터 플레인 호출이 기록된다. 정상 접속 경로에서는 ListLoginProfiles와 CheckPolicy가 연속적으로 발생하는 반면, 권한이 없는 사용자에 의한 접속 시도에서는 CheckPolicy 로그만 발견된다. 그림 3은 권한이 없는 사용자가 외부에서 SSH 접속을 시도했을 때 나타나는 로그이다.



(그림 3) Opensearch 탐지 결과

5. 결론

본 연구는 AWS Amplify, Azure Synapse, GCP OS Login 세 가지 보안 사건을 대상으로, 각 사례에 대해 예방 및 탐지 도구를 매핑하고 파이프라인 관점에서 이를 검증하였다. 그 결과, 정책 및 코드 기반의 점검은 초기 단계에서 취약한 신뢰 정책을 효과적으로 차단할 수 있었고, 운영 단계에서는 권한 남용이나 비정상 로그인을 포함한 실행을 탐지할 수 있음을 확인하였다. 그러나 단일 도구만으로는 모든 계층을 탐지하기 어려워, 계층 간 공백이 발생할 수 있음을 확인하였다. 따라서 배포 전과 배포 이후 단계에서 여러 도구 조합을 통해 보안 파이프라인을 구성하는 것이 필요하다는 결론을 도출하였다.

향후 연구에서는 다양한 보안 사건과 오픈소스 도구를 대상으로 범위를 확장하고, 각 클라우드 플랫폼의 실제 운영 환경과 유사한 조건을 갖춘 실험 환경을 구성하여 연구를 수행할 계획이다.

Acknowledge

본 논문은 과학기술정보통신부의 재원으로 실감콘텐츠핵심기술개발
(Project No. RS-2023-00228996,40%), 한국연구재단(NRF) 중견후속
연구사업(Project No. RS-2023-00208460, 30%), 한국콘텐츠진흥원(KOCCA) 저작권기술 글로벌 인재양성사업 (Project No. RS-2025-02221620, 30%)의 지원을 받아 수행된 연구임.

참고문헌

[1] Aljahdali, H., Walters, R. J., and Wills, G. B., Multi-tenancy in Cloud Computing, Proceedings of the 8th International Symposium on Service-Oriented System Engineering (SOSE), Oxford, UK, 2014, pp. 344 - 351.

[2] Kazdagli, M., Tiwari, M., and Kumar, A., Leveraging AI Planning for Detecting Cloud Security Vulnerabilities, arXiv preprint arXiv:2402.10985, 2024.

[3] Di Cao1, Yong Liao1, Xiuwei Shang,, “RealVul: Can We Detect Vulnerabilities in Web Applications with LLM?” arXiv preprint arXiv:2410.07573, 2024.

[4] Manzoor, A., Zhong, Y., Karim, M. R., “Comprehensive Comparative Analysis of Open-Source SIEM Solutions for Scalable Security Management in Small and Medium Enterprises,” PLOS ONE, Vol. 19, No. 1, e0301183, 2024.

[5] Mohammed, T., Khan, M. A., Razaque, A., and Nasir, Q., "Evaluating security and performance of open-source SIEM solutions", PLOS ONE, vol. 18, no. 9, e0301183, 2023.

[6] Asad, H., Adhikari, S., Gashi, I., “A perspective - retrospective analysis of diversity in signature-based open-source network intrusion detection systems,” International Journal of Information Security, Vol. 23, pp. 1331 - 1346, 2024.

[7] Ranjan, P., Jha, R. K., and Singh, D., "A perspective - retrospective analysis of diversity in signature-based network IDSs", International Journal of Information Security, vol. 23, no. 2, pp. 123 - 138, 2023.

[8] Kumar, A., "Evaluating Falco for real-time detection in Kubernetes environments", Proceedings of the 2022 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Bangkok, Thailand, 2022, pp. 132 - 139.

[9] Maqueda, V., and López, J., "Security in Cloud Native Services: A Survey", Journal of Cybersecurity and Privacy, vol. 3, no. 4, pp. 698 - 716, 2023.

[10] Amazon Web Services, “CVE-2024-28056,”AWS Security Bulletin AWS-2024-003, Apr. 15, 2024.

[11] Microsoft Security Response Center (MSRC), “Vulnerability mitigated in the third-party Data Connector used in Azure Synapse Pipelines and Azure Data Factory (CVE-2022-29972),” May 9, 2022.

[12] National Vulnerability Database (NVD), “CVE-2025-2903 Detail,” Apr. 17, 2025.

[13] Open Policy Agent (OPA) Contributors, OPA (Open Policy Agent), 소프트웨어, GitHub,

[14] Duo Labs, Parliament: AWS IAM linting library, 소프트웨어, GitHub, 2025.

[15] Bridgecrew, Checkov, 소프트웨어, GitHub, 2025.

[16] Falco Security, Falco Website (project docs source), 소프트웨어, GitHub, 2025.

[17] Checkmarx, KICS (Keeping Infrastructure as Code Secure), 소프트웨어, GitHub, 2025.

[18] OpenSearch Project, opensearch-cli, 소프트웨어, GitHub, 2025.