오픈소스 클라우드 보안 도구 비교 분석 및 통합 활용 전략 연구

김도영*, 공나영*, 최상훈[1], 박기웅†

세종대학교 Syscore Lab. (학부생, 연구교수[1])
**세종대학교 정보보호학과 (교수†)

A Study on the Comparative Analysis and Integrated Utilization Strategy of Open-Source Cloud Security Tools

Do-Yeong Gim*, Na-Young Kong*, Sang-Hoon Choi[1], Ki-Woong Park†

* SysCore Lab., Sejong University
**Dept. of Computer and Information Security, Sejong University
(Undergraduate student*, Research Professor[1], Professor†)

요 약

클라우드 컴퓨팅은 기존 환경과 다른 새로운 보안 과제를 제시하며, 2023년 대비 침해 사고가 136% 증가했다. 대부분의 공격은 잘못된 구성, 복잡한 IAM, 가시성 부족 등 운영상의 취약점을 악용한다. 이에 대응하기 위해 다양한 오픈소스 보안 도구가 등장했으나, 실무자가 실용성에 대해 체계적으로 평가하고 선정할 기준은 부족하다. 본 연구에서는 실제 공격자의 전술, 기술, 절차(TTPs)를 체계화한 MITRE ATT&CK for Cloud 프레임워크를 분석 기준으로 채택하여 공격과 방어 역할을 대표하는 네 가지 주요 오픈소스 클라우드 보안 도구(Pacu, CloudFox, Prowler, ScoutSuite)의 기능과 전략적 가치를 비교 평가한다. 분석 결과 각 도구는 상호 배타적인 관계가 아닌 보완적인 역할을 수행함을 확인하였다.

I. 서론

클라우드 컴퓨팅으로의 전환은 현대 정보 기술 환경의 패러다임 변화를 이끌었다. 하지만 클라우드 환경의 도입은 디지털 공격 표면을 확장시켜 전통적인 온프레미스 환경과는 다른 새로운 보안 과제를 제시한다. 이로 인해 발생하는 보안 위협은 정교해지고 복잡해지고 있다. CrowdStrike 조사에 따르면 2025년 상반기에 클라우드 환경에서 탐지된 침해 사고는 2023년 대비 136% 증가했으며 대부분의 공격은 클라우드 환경의 고유한 특성을 악용하는 형태로 이루어졌다[1].

클라우드 환경의 핵심적인 취약점은 기술 자체의 결함보다는 잘못된 구성, 복잡한 신원 및 접근 관리(IAM), 동적인 워크로드에 대한 가시성 부족 등 운영상의 문제에서 비롯되는 경우가 많다. 실제로 Orca Security의 조사에 따르면 전체 클라우드 자산의 32%가 관리가 미흡한 상태로 방치되고 있으며 전체 조직의 90%가 인터넷에서 직접 접근 가능한 방치된 자산을 보유하고 있는 것으로 나타났다[2]. 클라우드 보안 위협의 증가에 대응하기 위해 다양한 감사 도구가 개발되고 배포되고 있다. 그러나 보안 실무자들은 많은 도구 중 어떤 것을 선택할지에 대한 명확한 기준 없이 개별 도구의 기능 목록이나 단편적인 정보에 의존하는 경우가 많다. 따라서 본 논문은 클라우드 감사 도구들의 기능을 실제 위협 시나리오에 기반하여 체계적으로 비교 분석하고 이를 통해 상호보완적인 통합 활용 전략을 제안한다.

† 교신저자: 박기웅 (세종대학교 정보보호학과 교수)
본 논문은 과학기술정보통신부의 재원으로 실감콘텐츠핵심기술개발(Project No. RS-2023-00228996, 40%), 국방ICT융합연구(Project No. 2022-11220701, 30%), 한국콘텐츠진흥원(KOCCA) 저작권기술 글로벌 인재 양성사업 (Project No. RS-2025-02221620, 30%)의 지원을 받아 수행된 연구임.

<표 1> 클라우드 보안도구 별 전략적 역할 및 기술적 특징

구분	Pacu	CloudFox	Prowler	ScoutSuite
유형	공격/침투	공격/정찰	방어/감사	방어/감사
주요 기능	AWS 환경 내 권한 상승, 백도어 설치 등 실제 공격 수행	클라우드 환경의 공격 표면 및 경로 탐색, 상황 인식	보안 설정 오류 탐지, 컴플라이언스 준수 여부 지속적 모니터링	특정 시점의 클라우드 계정 보안 상태 평가 및 위험 영역 식별
지원 클라우드	AWS	AWS, Azure, GCP	AWS, Azure, GCP, Kubernetes 등	AWS, Azure, GCP, OCI 등
MITRE ATT&CK 전술	Execution, Privilege Escalation, Defense Evasion, Persistence	Initial Access, Discovery	전술 전반의 설정 오류 탐지	전술 전반의 설정 오류 탐지

본 논문의 구성은 다음과 같다. 2장에서는 클라우드 보안 및 분석 프레임워크 배경지식 및 선행 연구를 살펴본다. 3장에서는 본 연구에서 선정한 감사 도구들을 비교 분석하고 통합 활용 전략을 제안한다. 마지막으로 4장에서는 결론 및 향후 연구 방향을 기술한다.

II. 배경지식 및 관련 연구

2.1 클라우드 감사 도구

본 논문에서는 클라우드 보안 도구별 다른 전략적 역할을 수행하는 대표적인 네 가지 감사 도구를 분석하였다.

Pacu는 AWS 환경에 특화된 공격적 침투 프레임워크로 초기 접근에 성공한 공격자가 후속 공격 단계를 정교하게 시뮬레이션하는 데 초점을 맞춘다. MITRE는 Pacu를 공식적인 공격 도구(Software ID: S1091)로 인정하고 있다.

CloudFox는 다중 클라우드 환경에서 활용 가능한 공격적 정찰 도구로 복잡한 환경 내에서 잠재적인 공격 경로를 신속하게 식별하고 공격 표면을 가시화하는 것을 목적으로 한다. CloudFox는 공격의 초기 단계인 탐지 및 정찰 전술을 효과적으로 지원한다.

Prowler와 ScoutSuite는 방어적 보안 감사 도구로 특정 공격 기술의 성공 가능성을 높이는 시스템의 설정 오류나 취약점을 탐지하는 데 초점을 맞추어 개발되었다.

2.2 클라우드 보안 취약점 분석 연구

클라우드 컴퓨팅의 보안 문제를 해결하기 위한 다수의 연구는 클라우드 환경의 고유한 보안 위협과 취약점을 분석하고 이에 대응하기 위한 기술적, 정책적 방안을 제시하는 데 초점을 맞추고 있다. 김아용의 연구에서는 클라우드 도입 시 가장 큰 문제점으로 개인 정보 유출을 지적하며 클라우드 보안 기술과 취약점을 분석하여 보안 향상 방안을 제안했다[3].

2.3 MITRE ATT&CK 프레임워크 활용 연구

본 연구의 분석 기준으로 사용된 MITRE ATT&CK 프레임워크는 다양한 실무 및 연구에서 활용되고 있다. Panaousis의 연구에서는 417개의 논문을 분석하여 MITRE ATT&CK 프레임워크가 실제 공격 사례를 기반으로 적대적 행위를 체계적으로 모델링하여 위협 인텔리전스, 침해 사고 대응, 보안 취약점 우선순위 선정 등 다양한 영역에서 프레임워크가 효과적으로 활용될 수 있음을 체계적으로 증명했다[4].

III. 클라우드 감사 도구 분석

본 연구는 분석적 일관성과 깊이를 확보하기 위해 MITRE ATT&CK for Cloud를 채택했다. MITRE ATT&CK은 실제 관측된 공격 사례를 바탕으로 공격자의 전술, 기술, 절차(TTPs)를 체계적으로 정리한 지식 베이스다. 해당 프레임워크가 실제 공격 데이터를 기반으로 구축되어

실증적 증거에 근거하며 서로 다른 목적을 가진 보안 도구의 기능을 동일한 기준으로 비교 평가할 수 있는 공통의 기준점을 제공하기 때문에 본 연구에 적합하다고 판단하였다.

3.1 도구별 기능 및 특성 분석

각 도구의 전략적 역할과 기술적 특성을 MITRE ATT&CK 프레임워크 기준으로 비교하면 <표 1>과 같다. 각 도구는 뚜렷한 전략적 포지션을 가지고 있다. 공격적 도구인 Pacu와 CloudFox는 각각 공격의 깊이와 넓이를 담당하며 실제 위협을 시뮬레이션하고 공격 표면을 가시화하는데 필수적이다. 방어적 도구인 Prowler와 ScoutSuite는 정적 구성 분석을 통해 보안 기준 준수 여부를 평가하고 잠재적 위험을 사전에 식별한다. 공격적 도구와 방어적 도구는 상호보완적 관계를 형성한다.

3.2 전략적 시사점

가장 중요한 시사점은 다양한 감사 도구 생태계가 통합적으로 활용될 때 그 가치가 극대화된다는 점이다. 공격과 방어 도구의 상호보완적 특성을 결합하면 지속적인 보안 강화 사이클을 구축할 수 있다. 이 과정은 다음과 같은 피드백 순환 구조를 통해 구현될 수 있다.

첫째, 방어적 감사를 통한 기준선 설정이다. Prowler나 ScoutSuite와 같은 방어적 감사 도구를 사용하여 전체 클라우드 환경에 대한 포괄적인 보안 감사를 수행한다. 이를 통해 현재의 보안 설정 오류, 규정 미준수 항목, 잠재적 취약점을 식별하고 이를 해결하여 초기 보안 기준선을 설정하고 시스템을 강화할 수 있다.

둘째, 공격 시뮬레이션을 통한 검증이다. CloudFox를 사용하여 강화된 환경에 여전히 남아 있는 공격 표면과 잠재적 침투 경로를 탐색한다. 이 과정에서 식별된 고위험 경로에 대해 Pacu를 사용하여 실제 공격을 시뮬레이션한다. 이 단계의 목표는 이론적인 취약점이 실제로 악용 가능한지를 검증하는 것이다.

마지막으로, 분석 및 개선을 통한 방어 고도화이다. 공격 시뮬레이션의 결과를 분석하여 기존 방어 및 탐지 체계의 효율성을 평가한다. 이 분석 결과를 바탕으로 방어 설정을 더욱 정교하게 조정하여 모니터링 규칙을 개선하며 새로운 사용자 정의 규칙을 Prowler에 추가하여 유사한 공격 패턴을 탐지할 수 있다.

IV. 결론

클라우드 컴퓨팅의 확산은 IT 운영의 패러다임을 변화시켰지만 잘못된 구성과 복잡한 IAM, 가시성 부족 등 운영상의 취약점을 악용하는 새로운 보안 위협을 급격히 증가시켰다. 이에 따라 다양한 보안 감사 도구가 등장했으나 실무자들이 이를 체계적으로 평가하고 효과적으로 통합할 기준은 부재하다. 본 연구에서는 클라우드 컴퓨팅 환경의 보안 위협에 대응하기 위한 보안 감사 도구의 역할을 체계적으로 분석하였다. MITRE ATT&CK for Cloud 프레임워크를 기준으로 공격 및 방어 도구를 비교 분석함으로써 개별 도구의 독립적인 사용을 넘어 이들을 연계한 상호보완적인 통합 활용 전략이라는 구체적이고 실용적인 전략을 제안하였다. 향후 연구에서는 제안한 통합 활용 전략의 자동화 프레임워크 개발을 수행할 예정이다.

[참고문헌]

[1] CrowdStrike, 2025 Threat Hunting Report, CrowdStrike, 2025.

[2] Orca Security, 2022 State of Public Cloud Security Report, Orca Security, 2022.

[3] Ahyoung Kim, Sungok Lee, Seunghan Ryu, and Hoikyung Jeong, Cloud Security Technology and Vulnerability Assessment, KIISE, May, 2013.

[4] Emmanouil Panaousis, et al., SoK: The MITRE ATT&CK Framework in Research and Practice, arXiv:2304.07411, Apr. 2023.

[5] The MITRE Corporation, MITRE ATT&CK®, The MITRE Corporation, 2025.

[6] The MITRE Corporation, Pacu, Software S1091, MITRE ATT&CK®, Oct. 2023.

[7] Prowler Cloud, Prowler, GitHub, 2025.

[8] NCC Group, ScoutSuite, GitHub, 2025.