멀티 클라우드 보안 운영 효율화를 위한 통합 심각도 매핑 모델 연구

공나영*, 김도영*, 최상훈[1], 박기웅†

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

A Study on an Integrated Severity Mapping Model for Efficient Multi-Cloud Security Operations

Na-Young Kong*, Do-Yeong Gim*, 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

최근 클라우드의 유연성과 비용 효율성을 극대화하기 위해 여러 클라우드 서비스 제공업체의 인프라를 병행 활용하는 멀티 클라우드 전략이 확산되고 있다. 그러나 이기종 클라우드 환경에서는 로그 구조와 위험 심각도 분류 체계가 상이하여, 침해사고 발생 시 신속하고 일관된 대응이 어렵다는 한계가 존재한다. 본 연구에서는 국내외 주요 CSP의 심각도 분류 모델을 비교 분석하여 상태, 영향, 악용 가능성 등의 요소를 반영한 3단계 통합 심각도 모델과 매핑 규칙을 제안한다. 제안된 모델은 SIEM 및 SOAR 플랫폼에 연계되어 위협 정보의 정규화 및 자동화된 대응을 가능하게 한다. 본 연구는 이기종 클라우드 환경에서 위협 정보의 일관성을 확보하고, 통합 보안 운영의 기반을 마련한다.

I. 서론

최근 클라우드의 유연성, 비용 효율성 및 벤더 종속성 회피 이점을 활용하기 위해 멀티 클라우드를 도입하는 조직이 늘고 있다. 멀티 클라우드란 두 개 이상의 클라우드 서비스 제공업체의 인프라와 서비스를 활용하는 전략이다[1]. 그러나 멀티 클라우드 환경에서는 로그 구조와 위험 심각도 분류 체계에 차이가 있어 침해사고 발생 시 신속하고 체계적인 대응이 어렵다[2]. 이에 본 연구는 보안 운영의 효율성을 높이기 위해 이기종 클라우드 환경의 상이한 위험 심각도 분류 체계를 통합하는 것을 목표로 한다. 단순히 형식을 맞추는 것을 넘어, 위협에 대한 신속하고 일관된 대응을 가능하게 하는 로그 분석 및 통합의 핵심 기반을 구축하는 데 목적이 있다.

본 논문의 구성은 다음과 같다. 2장에서 클라우드 벤더별 심각도 모델을 비교하고, 3장에서는 멀티 클라우드 환경을 관리하기 위한 모델을 제안한다. 4장에서는 구현 요구사항을 설명하고, 5장에서는 결론 및 향후 연구를 기술한다.

II. 클라우드 벤더별 심각도 모델 비교

2.1 국외 클라우드 제공업체

국외 Cloud Service Provider(CSP)는 판독이 용이한 구조화된 위협 탐지 데이터를 제공한다. 이는 통합 심각도 분류 모델의 기준선이 된다.

2.1.1 Amazon Web Services (AWS)

AWS GuardDuty는 AWS 환경 전반에서 악

†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.

의적인 활동과 무단 동작을 모니터링하도록 설계된 위협 탐지 서비스이다. 각 GuardDuty 결과에는 심각도 수준과 값이 할당된다. 심각도 값은 1.0에서 10.0 사이의 범위에 속하며, 값이 높을수록 보안 위협이 더 높음을 나타낸다. 범위를 Critical(9.0-10.0), High(7.0-8.9), Medium(4.0-6.9), Low(1.0-3.9)로 구분한다[3]. 탐지 결과는 AWS CloudTrail 로그에 기록된 API 호출에 기반한다.

2.1.2 Google Cloud Platform (GCP)

Security Command Center는 Google Cloud의 중앙 집중식 취약점 및 위협 보고 서비스이다. SCC는 심각도를 Critical, High, Medium, Low로 구분하며, 이는 취약점의 악용 가능성에 중점을 둔다[4]. SCC 탐지 결과의 근거는 Cloud Audit Logs이다.

2.1.3 Microsoft Azure

Microsoft Sentinel은 클라우드 네이티브 보안 정보 및 이벤트 관리(SIEM) 및 보안 오케스트레이션, 자동화 및 대응(SOAR) 솔루션이다. 심각도는 High, Medium, Low, Informational로 구분한다[5]. Sentinel 분석 규칙의 주요 입력 데이터는 Azure Activity Log이다.

2.2 국내 클라우드 제공업체

국내 CSP는 이벤트 분석을 통해 위험도를 추론해야 하는 관리적 서비스 중심의 접근 방식을 취한다. 이러한 접근 방식의 차이는 멀티 클라우드 환경에서 심각도 분류의 일관성을 확보하는 데 방해요소로 작용할 수 있다.

2.2.1 Naver Cloud Platform (NCP)

NCP는 Security Monitoring과 Cloud Activity Tracer라는 두 가지 보안 서비스를 제공한다[6]. 이 중 Security Monitoring은 Managed 서비스 형태로 운영된다. 이는 다양한 탐지 솔루션에서 생성된 로그를 처리하여 분석 보고서를 제공한다.

2.2.2 KT Cloud

KT Cloud DC 보안관제를 통해 모니터링 되는 관리형 보안 서비스를 제공한다. 심각도는 보안 보고서나 침해 사고 분석 결과를 통해 전달되는 형태로 제공된다[7].

2.2.3 NHN Cloud

Security Monitoring 서비스를 운영하여 IDS/SIEM 패턴을 기반으로 관제 서비스를 제공한다. NHN CloudTrail은 소스, 서비스, 사용자 별로 이벤트를 기록하는 감사 로그 역할을 수행한다. 심각도는 관제 서비스를 통해 분석 결과 형태로 제공된다[8].

III. 멀티 클라우드 환경을 위한 통합 심각도 모델

3.1 침해사고 대응을 위한 심각도 모델 설계

멀티 클라우드 환경의 복잡성을 효과적으로 관리하기 위해 3단계로 구성된 통합 심각도 모델을 제안한다. 통합 모델의 각 단계는 앞서 분석한 벤더별 심각도 모델의 상태, 영향, 악용 가능성, 이벤트 유형 등을 종합하여 다음과 같이 정의된다.

자원의 확정된 침해상태, 공격자가 광범위한 영향을 미칠 수 있는 권한을 획득한 상태, 즉시 악용 가능한 치명적인 취약점이 발견된 경우 High로 구분한다. High로 구분된 경우에는 즉각적인 자동화 대응 또는 격리 및 차단 조치를 요구한다.

정상적인 행위에 벗어나는 활동이 탐지되거나, 자원 침해의 가능성이 있는 경우, 취약점 악용을 위해 여러 단계의 공격이 필요한 경우 Medium로 구분한다. Medium로 구분된 경우에는 가급적 빠른 시간 내에 조사를 필요로 한다.

공격 시도가 있었으나 차단되었거나 실패한 경우, 자원을 직접적으로 노출시키지는 않으나 가시성을 저해하거나 향후 공격에 활용될 수 있는 이벤트인 경우 Low로 구분한다. 즉각적으로 조치는 불 필요하지만 분석을 위한 로깅을 통해 보안 강화에 활용한다.

3.2 벤더별 심각도와 통합 모델 매핑

벤더별 심각도를 분석하여 매핑한 결과는 <표1>과 같다.

<표 1> 국내외 CSP 별 심각도 분류

벤더	심각도/이벤트 유형	통합 심각도
AWS	Critical	High
AWS	High	High
AWS	Medium	Medium
AWS	Low	Low
GCP	Critical	High
GCP	High	High
GCP	Medium	Medium
GCP	Low	Low
Azure	High	High
Azure	Medium	Medium
Azure	Low	Low
Azure	Informational	Low
NCP	DDoS 공격 탐지/차단	High
NCP	IPS/WAF 차단, 악성코드 탐지	Medium
NCP	IDS 경보	Low
KT Cloud	DDoS 공격 탐지/차단	High
KT Cloud	IPS/WAF 차단	Medium
KT Cloud	IDS 경보	Low
NHN Cloud	침해 사고 발생	High
NHN Cloud	IDS/SIEM 패턴 매칭	Medium
NHN Cloud	보안 취약점 공지	Low

IV.모델 적용을 위한 요구사항

통합 심각도 모델이 보안 정보 및 이벤트 관리(SIEM)와 보안 오케스트레이션, 자동화 및 대응(SOAR) 플랫폼과 연계하여 운영될 때 가치가 극대화된다. SIEM은 통합 심각도 모델을 통해 심각도를 동일한 단계로 표현함으로써 분석 효율성을 높인다. 이를 통해 보안 분석가는 일관된 기준으로 위협을 탐지하고 대응할 수 있다. SOAR는 정규화환 경고 데이터를 기반으로 자동화된 대응을 수행한다. SIEM이 통합한 경고가 감지되면 SOAR는 사전에 정의된 플레이북을 실행하여 대응 절차를 자동으로 수행한다. 이러한 자동화는 침해 사고 대응 평균 시간을 단축하고 피해 확산을 최소화한다.

V. 결론

최근 클라우드 도입이 확산되면서, 유연성과 비용 효율성을 극대화하기 위해 여러 CSP를 병행하는 멀티 클라우드 환경이 보편화되고 있다. 그러나 이기종 클라우드 간 로그 구조와 심각도 체계의 불일치로 인해 침해사고 대응의 일관성이 저하되는 문제가 있다. 본 연구에서는 국내외 CSP의 보안 로깅 및 심각도 분류 체계를 비교 분석하였다. 이러한 분석을 바탕으로 상이한 위협 정보를 표준화된 언어로 변환하기 위한 해결책으로서 High, Medium, Low 3단계의 통합 심각도 모델과 매핑 규칙을 제안하였다. 이 프레임워크는 SIEM 및 SOAR 플랫폼에 적용되어 위협 정보의 일관성을 확보하고, 자동화된 대응을 가능하게 함으로써 침해 사고 대응 시간을 단축시키는 데 기여할 수 있다.

향후 연구에서는 현재 High, Medium, Low로 단순화된 심각도 매핑 과정에서 발생할 수 있는 중요 정보 누락 문제를 해결하기 위해, 국내 CSP별 로그 특성과 업데이트 정책을 반영하여 통합 심각도 모델의 정밀도를 향상시키고, 제로데이 및 미확인 위협에 대응할 수 있는 자동화된 보안 운영 체계로의 확장을 수행할 예정이다.

[참고문헌]

[1] K.J.P.E.K.Almutairi and R.Q.M.Alharbi, A survey of multi-cloud computing architectures and issues, IOP Conf. Series: Materials Science and Engineering, vol.1098, no.4, pp.042001, Aug, 2021.

[2] A. Yeboah-Ofori, A. Jafar, T. Abisogun, I. Hilton, W. Oseni and A. Musa, Data Security and Governance in Multi-Cloud Computing Environment, Proc. 2024 11th International Conference on Future Internet of Things and Cloud (FiCloud), pp.215-222, Aug, 2024.

[3] Amazon Web Services (AWS), Severity levels of GuardDuty findings, Amazon GuardDuty User Guide, 2025.

[4] Google Cloud, Finding severities, Security Command Center, 2025.

[5] Microsoft, Scheduled analytics rules in Microsoft Sentinel, Microsoft Learn, 2024.

[6] NAVER Cloud Platform, Cloud Activity Tracer overview, NAVER Cloud Platform User Guide, 2025.

[7] Kt cloud, 보안 서비스, kt cloud DC, 2025.

[8] NHN Cloud, CloudTrail Console Guide, NHN Cloud User Guide, 2025.