한국정보보호학회
Korea Institute of Information Security & Cryptology

Proceedings

2021년 한국정보보호학회 하계학술대회

CISC-S'21

Conference on Information Security and Cryptography Summer 2021

2021년 6월 24일(목)

온라인 컨퍼런스

(개회식 촬영: 한국과학기술회관 12F 아나이스홀)

주최 한국정보보호학회 Korea Institute of Information Security & Cryptology

주관 KAIST 한국과학기술원

후원 과학기술정보통신부 국가정보원 National Intelligence Service Korea 행정안전부

NSR 국가보안기술연구소 National Security Research Institute KISA 한국인터넷진흥원 ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute

쌍용정보통신주식회사 SsangYong Information & Communications Corp.

상용 클라우드 서비스 대상 내부 자원 모니터링 및 보안 위협 커버리지 분석

조여름*, 박기웅†

*세종대학교 시스템보안 연구실, †세종대학교 정보보호학과

A Coverage Analysis of Internal Resource Monitoring and Security Threats for Commercial Cloud Service

Yeo-Reum Jo*, Ki-Woong Park†

* SysCore Lab., Sejong University.

†Department of Computer and Information Security, Sejong University

요 약

클라우드가 활성화되면서 기업 및 공공기관도 인프라를 클라우드로 이전하려는 움직임이 가속화 되고 있다. 클라우드 활용범위가 확대됨에 따라 클라우드에 대한 보안의 중요성이 대두되고 있다. 클라우드는 다수의 사용자가 물리적인 자원을 공유하고, 다양한 서비스가 구동되기 때문에 복잡한 구조를 가지며 이러한 구조는 잠재적인 보안 위협을 발생시킨다. 따라서 클라우드 인프라의 안정성을 강화하기 위해서 보안 위협을 탐지할 수 있는 방안이 도출되어야 한다.

본 논문에서는 클라우드 환경의 보안 위협과 상용 클라우드 서비스 제공사의 모니터링 및 보안 위협 탐지 기술의 조사를 통해 보안 커버리지를 분석하였다. 본 논문에서 도출한 커버리지 분석 결과는 클라우드 사용자와 조직에 적합한 보안 아키텍처 설계에 활용될 수 있다.

I. 서론

클라우드 서비스가 활성화되면서 기업 및 공공기관도 클라우드로 이전하려는 움직임이 가속화 되고 있다. 다수의 사용자가 물리적인 자원을 공유하고, 다양한 서비스가 구동되기 때문에 복잡한 구조를 가지며 이러한 구조는 잠재적인 보안 위협을 발생시킨다. 따라서 클라우드 인프라의 안정성을 강화하기 위해서 보안 위협을 탐지할 수 있는 방안이 필요하다.

클라우드 서비스 제공사는 클라우드 환경의 내부 자원을 모니터링하고, 보안 위협을 탐지하는 서비스를 제공하고 있다 [1-9]. 각 제공사의 서비스마다 제공하는 모니터링 지점과 보안 위협에 대한 커버리지는 상이하기 때문에 사용자는 이를 파악하여 적합한 보안 아키텍처를 수립하고 능동적인 대응 전략을 세워야 한다.

본 논문에서는 클라우드 환경의 보안 위협과 해당 위협과 관련된 리소스를 분석하고 클라우드 서비스 제공사의 내부 자원 모니터링과 보안 위협 탐지 커버리지를 측정 및 분석한다.

본 논문의 구성은 다음과 같다. 2장에서는 클라우드 보안 위협과 해당 탐지 리소스를 분석한다. 3장에서는 클라우드 서비스 제공사가 제공하는 클라우드 보안 위협 탐지 커버리지를 측정 및 분석한다. 그 결과를 바탕으로 4장에서 결론을 도출한다.

†교신저자: 박기웅 (세종대학교 정보보호학과 교수)

본 논문은 ETRI부설연구소의 위탁연구과제[2021-086]의 지원(50%)과 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원(No.2019-0-00273, 25%) 및 한국연구재단(No.NRF-2020R1A2C4002737, 25%)의 지원을 받아 수행된 연구임.

II. 클라우드 보안 위협

클라우드 보안의 범위는 클라우드 환경의 하드웨어부터 사용자의 데이터까지 이른다. 이 장에서는 클라우드 환경에서 발생하는 주요 보안

[표 1] 클라우드 보안 위협 분류

		보안 책임		Architecture			
		고객	CSP	Appli	Info	Meta	Infra
클라우드 보안 위협	데이터 유출(a)	○	○	○	○	○	○
	불충분한 액세스 관리(b)	○					○
	잘못된 보안 설정(c)	○		○	○	○	○
	내부자 위협(d) (클라우드 사용자)	○					○
	계정 탈취(e)	○	○	○		○	
	클라우드 서비스 악용(f)	○	○	○		○	○
	불안정한 인터페이스와 API(g)	○	○	○		○	○
	내부자 위협(h) (클라우드 제공사)		○				○

위협을 조사하고 해당 위협의 대응 방안과 탐지 리소스를 분석한다. 또한, 클라우드 보안 위협 개념도를 통해서 조사한 위협 지점을 나타낸다.

2.1 클라우드 보안 위협과 모니터링 리소스

- 데이터 유출(a) : 클라우드에 저장된 개인 정보, 신용 정보 등의 민감한 데이터가 외부로 유출되는 것을 말한다. 민감한 데이터를 식별하고 접근 권한을 최소화하며 사용자의 의심스러운 데이터 접근을 탐지한다.
- 불충분한 액세스 관리(b) : 접근 관리가 미흡하여 인가되지 않은 사용자가 클라우드 리소스에 접근하는 것을 의미한다. 사용하지 않는 신원과 접근 권한, 작업 종료 및 역할 전환과 같은 자격 변경 등의 모니터링을 통해 접근 권한을 최소화한다.
- 잘못된 보안 설정(c) : 클라우드 데이터 및 서비스 보호를 위한 적절한 보안 설정을 하지 못하는 것을 의미한다. 인스턴스 설정 변경 로그, 보안 설정 로그와 같은 구성 로그와 잘못 설정된 리소스를 지속적으로 수집하고 감시한다.
- 내부자 위협(클라우드 사용자)(d) : 접근 권한을 가지는 내부자가 악의적이거나 의도하지 않은 방식으로 조직의 자산에 악영향을 미치는 것을 의미한다. 잘못 구성된 클라우드 리소스를 감시하고 비정상적인 패턴을 가지는 접속 등을 모니터링 한다.
- 계정 탈취(e) : 악의적인 외부자가 클라우드 접근 권한을 가지는 크리덴셜을 탈취하는 것을 의미한다. 계정 취약 여부를 지속적으로 점검하고 사용자의 접근 및 활동 로그에 대해 실시간으로 모니터링 한다.
- 클라우드 서비스 악용(f) : 클라우드를 이용하여 악의적인 활동을 하는 것을 의미한다. 사용자의 행위 분석, 사용자 정상 동작 정의 후 이상행위 탐지, 가상 머신 취약성을 점검한다.
- 불안정한 인터페이스와 API(g) : 클라우드 인터페이스와 API의 취약점으로 인해 발생하는 보안 위협이다. API 트래픽을 감시하고 사용자의 이상 행동을 탐지한다.
- 내부자 위협(클라우드 제공사)(h) : 클라우드 서비스 제공사의 내부자로 인해 발생하는 위협을 의미한다. 사용자의 인스턴스와 관련된 클라우드 제공사 관리자의 의심스러운 활동을 탐지한다.

[표 1]은 2장에서 조사한 클라우드 보안 위협 분석을 통해 보안 책임과 위협 대상 아키텍처를 정리한 표이다[10]. [표 1]과 분석한 보안 위협 탐지 리소스는 3장에서 커버리지 측정 시에 활용이 된다.

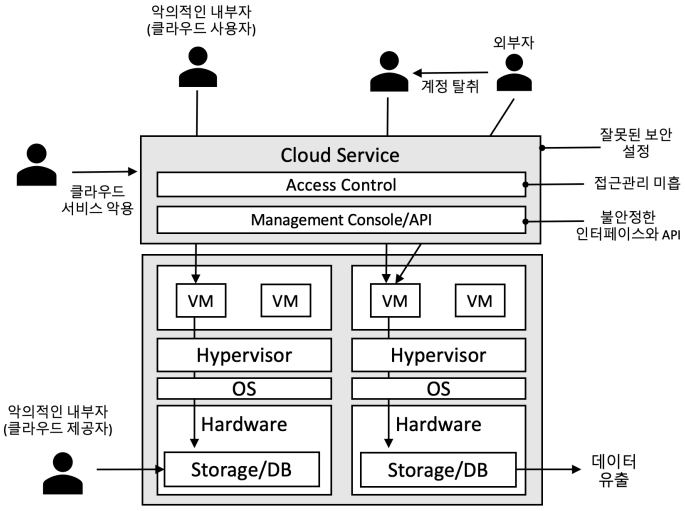
2.2 보안 위협 개념도

본 논문에서는 클라우드 보안 위협과 탐지 리소스 분석을 통해 클라우드 아키텍처의 보안 위협 개념도를 [그림 1]과 같이 구성하였다. 해당 개념도는 클라우드 서비스 제공사의 커버리지를 측정하고 모니터링 지점을 나타낼 수 있도록 확장할 수 있다.

III. 클라우드 서비스 제공사 모니터링 커버리지 분석

클라우드 모니터링은 클라우드 서비스 제공사와 사용자 모두에게 가장 중요한 작업이다[11]. 클라우드 서비스 제공사는 클라우드 환경의 잠재적인 보안 위협을 탐지하기 위한 다양한 보안 서비스를 제공하고 있다. 본 장에서는 상용 클라우드 서비스 제공사를 선정하여 각 제공사의 주요 모니터링과 보안 위협 탐지 서비스를 조사하고 커버리지를 분석한다.

3.1 AWS



[그림 1] 클라우드 보안 위협 개념도

- Amazon CloudWatch[1] : CPU, Memory, Disk I/O, Network 같은 클라우드 리소스와 AWS 기반 애플리케이션에 대한 모니터링 서비스이다. AWS의 다른 보안 제품과 연동하여 로그를 통합적으로 수집할 수 있다.
- AWS Config[2] : AWS 리소스의 구성 변경 사항을 지속적으로 모니터링하며 리소스 구성의 전반적인 규정 준수 여부를 감시한다. 리소스는 EC2 인스턴스, 보안 그룹, VPC, EBS 등이 있다.
- Amazon GuardDuty[3] : AWS 환경 내의 네트워크 활동, 데이터 액세스 패턴 및 계정 동작을 연속적으로 모니터링 한다. 수집하는 데이터는 API 로그, AWS 계정 활동 로그, VPC Flow 로그, DNS 로그, S3 데이터 액세스 로그 등이 있다.
- Amazon Macie[4] : 머신러닝 및 패턴 일치를 활용하여 S3에 저장된 데이터에서 민감 데이터를 식별하고 데이터의 보호 상태를 파악한다. 스캔한 버킷과 객체의 기록과 민감한 데이터 검색 작업의 모든 출력을 S3 버킷으로 자동 전송한다.
- AWS CloudTrail[5] : AWS 인프라에서 Management Console 작업과 API 호출 기록 등 계정 활동 로그를 수집하여 리소스 보안을 위협하는 비정상적인 계정 활동을 탐지한다.
- Amazon Inspector[6] : Agent를 기반으로 EC2 인스턴스의 보안 위협을 탐지하고 보안 수준을 진단한다. EC2 인스턴스에 대한 외부 액세스, 원격 루트 로그인 활성화 또는 취약 소프트웨어 버전 확인 등을 포함한다.

3.2 Azure

- Azure Monitor[7] : 애플리케이션의 성능 및 사용량, 인프라(VM, AKS, Azure Storage, DB 등) 그리고 네트워크를 모니터링 한다.
- Azure Security Center[8] : 클라우드 인프라 전체의 통합된 보안 관리를 제공한다. 클라우드 보안 태세 관리와 워크로드 보호가 핵심 요소이며 Azure의 서비스, 보안 정책 및 준수 정도 등을 모니터링하고 에이전트를 설치하여 서버 및 가상머신을 보호하는 기능을 포함한다.
- Azure Defender[9] : 가상머신, SQL 데이터베이스, 컨테이너 등의 각 서비스에 맞춘 보안 위협을 탐지하고 방어하는 기능을 제공한다. 스토리지의 Defender는 계정에 액세스하거나 악용하려는 비정상적이고 잠재적인 위협을 탐지한다.

3.3 보안 커버리지 분석

상용 클라우드 서비스인 AWS와 Azure가 제공하는 내부 자원 및 보안 위협 탐지 서비스를 조사하고 커버리지를 분석했다. [표 2]를 참고하여 분석 결과를 살펴보면 클라우드 제공사의

[표 2] 클라우드 서비스 제공사 커버리지 분석

	AWS						Azure		
	1	2	3	4	5	6	7	8	9
A			✔	✔				✔	✔
B									
C		✔	✔		✔	✔	✔	✔	✔
D			✔		✔		✔	✔	✔
E			✔						
F	✔		✔		✔	✔		✔	✔
G			✔		✔				
H									

보안 서비스마다 다른 커버리지를 가지며 클라우드 사용자 책임의 보안 위협에 대해서는 넓은 커버리지를 보이지만 클라우드 서비스 제공사 책임의 내부자 위협에 대해서는 커버리지가 부족하다.

IV. 결론

본 논문에서는 클라우드 환경의 보안 위협과 상용 클라우드 서비스 제공사의 모니터링 및 보안 위협 탐지 기술의 조사를 통해 보안 커버리지를 분석하였다. 분석 결과 클라우드 제공사의 보안 서비스마다 커버리지가 상이했다. 따라서 사용자는 이러한 특징을 파악하여 조직에 적합한 보안 아키텍처를 수립하고 능동적인 대응 전략을 세워야 한다. 또한, 클라우드 사용자 책임의 보안 위협에 대해서는 넓은 커버리지를 보이지만 클라우드 제공사 책임의 영역의 위협에는 가시성이 제공되지 않았다. 이러한 문제점을 해결하기 위해 향후 연구에서는 클라우드 서비스 제공사 자체에 대한 위협을 고려한 제로 트러스트 기반의 클라우드 보안 모델을 연구할 예정이다.

[참고문헌]

[1] AWS CloudWatch, https://aws.amazon.com/cloudwatch/

[2] AWS Config, https://aws.amazon.com/config/

[3] Amazon GuardDuty, https://aws.amazon.com/guardduty/

[4] Amazon Maice, https://aws.amazon.com/macie/

[5] AWS CloudTrail, https://aws.amazon.com/cloudtrail/

[6] Amazon Inspector, https://aws.amazon.com/inspector/

[7] Azure Monitor, https://azure.microsoft.com/ko-kr/services/monitor/

[8] Azure Security Center, https://docs.microsoft.com/ko-kr/azure/security-center/

[9] Azure Defender, https://docs.microsoft.com/ko-kr/azure/security-center/azure-defender

[10] CSA, Top Threats to Cloud Computing The Egregious 11, 2020

[11] Aceto, Giuseppe, et al. "Cloud monitoring: Definitions, issues and future directions." 2012 IEEE 1st International Conference on Cloud Networking (CLOUDNET). IEEE, 2012.