Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.2, Apr. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.2.263

클라우드 환경에서의 ATT&CK 매트릭스 기반 이벤트 로그 분석 프레임워크*

김 예 은,[1†] 김 정 아,[2] 채 시 윤,[2] 홍 지 원,[2] 김 성 민[3‡]
[1,2,3]성신여자대학교 (대학원생, 학생, 교수)

Event Log Analysis Framework Based on the ATT&CK Matrix in Cloud Environments*

Yeeun Kim,[1†] Junga Kim,[2] Siyun Chae,[2] Jiwon Hong,[2] Seongmin Kim[3‡]
[1,2,3]Sungshin Women's University (Graduate student, Undergraduate student, Professor)

요 약

클라우드 마이그레이션 증가와 함께 클라우드 컴퓨팅 환경에서의 보안 위협도 급증하고 있다. 이에 효율적인 사고 조사를 수행하기 위한 로그 데이터 분석의 중요성이 강조되고 있다. 클라우드 환경에서는 서비스 다양성과 간편한 리소스 생성 등의 특성으로 인해 대량의 로그 데이터가 생성된다. 이로 인해 사고 발생 시 어떤 이벤트를 조사해야 하는지 판단하기 어렵고, 방대한 데이터를 모두 확인하려면 상당한 시간과 노력이 필요하다. 따라서 데이터를 효율적으로 조사하기 위한 분석체계가 필요하다.

AWS(Amazon Web Services)의 로깅 서비스인 CloudTrail은 계정에서 발생한 모든 API 호출 이벤트 로그를 수집한다. 그러나 사고 발생 시 어떤 로그를 분석해야 하는지 판단하기 위한 인사이트 제공 역할은 부족하다. 본 논문에서는 Cloud Matrix와 이벤트 정보를 연계하여 사고 조사를 효율적으로 수행할 수 있도록 하고, 이를 기반으로 사용자 행위 로그 이벤트의 발생 빈도 및 공격 정보를 동시에 확인할 수 있는 자동화 분석 프레임워크를 제안한다. 이를 통해 ATT&CK Framework를 기반으로 주요 이벤트를 식별하고, 사용자 행위를 효율적으로 파악함으로써 클라우드 사고 조사에 기여할 것으로 기대한다.

ABSTRACT

With the increasing trend of Cloud migration, security threats in the Cloud computing environment have also experienced a significant increase. Consequently, the importance of efficient incident investigation through log data analysis is being emphasized. In Cloud environments, the diversity of services and ease of resource creation generate a large volume of log data. Difficulties remain in determining which events to investigate when an incident occurs, and examining all the extensive log data requires considerable time and effort. Therefore, a systematic approach for efficient data investigation is necessary.

CloudTrail, the Amazon Web Services(AWS) logging service, collects logs of all API call events occurring in an account. However, CloudTrail lacks insights into which logs to analyze in the event of an incident. This paper proposes an automated analysis framework that integrates Cloud Matrix and event information for efficient incident investigation. The framework enables simultaneous examination of user behavior log events, event frequency, and attack information. We believe the proposed framework contributes to Cloud incident investigations by efficiently identifying critical events based on the ATT&CK Framework.

Keywords: Cloud Computing, AWS CloudTrail, eventName, ATT&CK Matrix

Received(02. 19. 2024), Modified(03. 20. 2024), Accepted(03. 21. 2024)

* 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 ICT 혁신인재4.0 사업의 연구결과로 수행되었음(IITP)

† 주저자, yeuna119@kakao.com
‡ 교신저자, sm.kim@sungshin.ac.kr(Corresponding author)

I. 서 론

비대면 서비스 수요 급증과 함께 각 기업은 비즈니스를 위한 IT 인프라 운영 방식에 전환을 맞이하게 되었다. 네트워크, 서버 등 정보자산을 물리적 환경에 직접 구성하는 온프레미스(On-Premise)에서 벗어나, 필요한 만큼의 IT 인프라를 가져와 가상 환경에 구축하는 클라우드로의 전환이 가속화된 것이다. 실제 시장조사기관 가트너에 따르면 퍼블릭 클라우드 서비스 지출액이 2022년 4,910억 달러에서 2023년 5,973억 달러로 증가할 것으로 전망했다[1]. 수요에 따른 탄력적 운영의 비용 효율성이 높은 이점으로 기업의 많은 워크로드가 클라우드로 마이그레이션 되고 있지만, 사용자의 실수로 인한 환경 구성 및 설정 오류 등으로 인한 침해사고도 빈번히 발생하고 있다. 실제 2021년 10월 Facebook의 클라우드 구성 오류로 인해 29억 명의 Facebook, WhatsApp 및 Instagram 사용자가 6시간 이상 완전히 중단되기도 하였다[2]. 이러한 클라우드의 사고 분석을 위해 서비스에서 사고 시점에 발생한 이벤트와 관련 세부 사항이 담긴 로그를 분석하는 것은 중요하다[3]. 그러나 클라우드 환경에서는 데이터 저장을 위한 스토리지인 S3, 웹 트래픽 탐지 및 차단을 위한 WAF 등 자원 생성이 온프레미스에 비해 빈번하여 단시간에 생성되는 로그의 수가 많고 이를 장기간 보관할 경우 많은 양의 스토리지 자원이 필요하다. 또한, 호스트 내 사고 조사 방법론이 성숙한 기존 온프레미스 환경에서와 달리, 클라우드 환경에서는 새로운 유형의 침해사고가 발생하기도 한다.

현재 클라우드 환경에서 침해사고 발생 시 어떤 로그를 분석해야 하는지에 대한 가이드라인은 부족한 상황이며, 생성된 다수의 로그에서 사고 관련 이벤트 로그를 식별해 내기 어렵다. 따라서, 클라우드 환경에서 보안 사고를 효율적으로 조사하기 위해서는 로그 이벤트의 명확한 분류체계가 요구된다. 이를 통해 사고 분석 및 조사에 필요한 이벤트를 신속하게 식별하고, 조사 시간과 절차를 단축할 수 있어야 한다.

상용 클라우드 서비스 제공 업체들은 침해사고 대응 및 클라우드 인스턴스에 대한 보안 위협 탐지를 위해 자체적으로 로깅 서비스를 제공하고 있으며, 대표적으로는 Amazon 사의 CloudTrail[4], Microsoft 사의 Activity log[5]가 있다. 이중 클라우드 시장 점유율이 가장 높은 AWS의 CloudTrail은 계정의 API 호출 관련 자원 및 서비스 작업 기록을 추적할 수 있으며, 연결된 S3 버킷 스토리지에 로그 기록을 저장할 수 있다. 그러나 CloudTrail은 계정 및 서비스의 활동 API를 기록하는 역할을 제공하지만, 특정 사고의 주요 이벤트를 판단해 주는 인사이트는 제공하지 않는다. 따라서 사고 분석을 위해 추가적인 도구나 수단이 필요하다. AWS CloudWatch는 클라우드 환경에서 발생하는 다양한 애플리케이션을 모니터링하는 서비스로[6], AWS에서 발생한 이벤트를 수집하여 설정값 위반에 대한 경보를 제공한다. 예를 들어, 특정 API 호출 이벤트 횟수가 정상 범위를 벗어나거나 이상 패턴이 관찰된 경우와 같이 지표에 대한 임곗값을 설정하고, 알림을 설정할 수 있다. 그러나 임곗값 설정을 위해 필요하다고 판단할 주요 eventName 정보가 부족하므로, 전문가가 아니라면 이벤트 기반 경보 설정 기준을 결정하기 어려울 수 있다.

본 논문에서는 클라우드 환경에서의 사고 분석을 위한 로그 이벤트 분류체계를 수립하고 수집된 로그를 자동화하여 관리 및 기사화해 주는 프레임워크를 제안한다. 구현을 위해 대표적 클라우드 서비스인 AWS의 로그 수집 도구를 기준으로 프레임워크 개발을 수행하였다. 이때, AWS CloudTrail의 로깅 기록에서 확인 가능한 eventName은 발생한 이벤트의 유형을 나타내며, 해당 이벤트가 어떤 작업과 활동을 통해 생성되었는지 식별하는 데 중요한 역할을 한다. 이에 eventName과 서비스 소스의 연계를 통한 시각화 분석 프레임워크를 제안한다. 프레임워크는 다음과 같은 동작 흐름을 갖는다. 먼저, 분류체계를 수립하기 위해 다양한 소스로부터의 로그를 수집하는 환경을 구성한다. 이후, 로그에서 식별된 eventName과 관련 서비스 정보를 MITRE ATT&CK Cloud Matrix와 연결하여 침해사고와 관련된 주요 이벤트 로그 데이터를 데이터베이스에 저장한다. 이를 통해 이벤트 발생량을 직관적으로 판단할 수 있도록 하며, Tactics에 따른 이벤트 정보를 식별할 수 있다. 제안된 로그 분석 프레임워크를 통해 특정 사고 발생 시 대량의 로그 파일에서도 필요한 이벤트 및 자원 관련 로그 데이터를 쉽게 식별하고 추출할 수 있음을 보여주고자 하며, 클라우드 환경에서의 사고 로그 분석 및 조사 프로세스의 시간을 단축하는 데 기여할 것으로 기대한다.

논문의 구성은 다음과 같다. 먼저 2장과 3장에서는 배경지식과 관련 연구를 서술한다. 4장에서는 제안하는 로그 분석 프레임워크의 구조 및 동작 흐름에

관해 설명하고, 5장에서는 침투 테스트를 기반으로 생성된 이벤트의 매핑 결과를 평가한다. 이후, 6장에서는 결론 및 향후 연구 방향에 관해 서술한다.

II. 배경 지식

2.1 클라우드 보안 위협

최근 클라우드 인프라를 대상으로, 기존 온프레미스 환경에서 발생할 수 있는 서비스 거부(DDoS), 계정 하이재킹과 같은 위협과 더불어 미흡한 자격증명과 액세스 및 키 관리 문제 등으로 인한 관리적 보안 위협이 다수 발생하고 있다. International Journal for Electronic Crime Investigation (IJECI)에 발표된 “Security Issues and challenges in Cloud Computing” 과 Cloud Security Alliance(CSA)의 “Top Threats to Cloud Computing“에 따르면 최근 클라우드 환경에서 발생하는 사고 대부분은 외부 공격자로부터가 아닌 클라우드 사용자나 운영자의 실수로 인한 관리적 보안 위협이 증가하고 있음을 볼 수 있다[7,8]. Table 1.은 CSA에서 제공한 클라우드 환경의 주요 보안 위협 결과로, DDoS, 시스템 취약점 등 기술적인 원인보다 불충분한 ID, 액세스 및 키 관리, 안전하지 않은 인터페이스와 API 등 관리적 위협이 높은 순위에 있는 것을 볼 수 있다. 클라우드 환경에서 관리적 보안 위협은 권한 부여, 서비스 및 애플리케이션 구성, 자원 변경 등에 의한 문제를 나타낸다. 이러한 사고 분석 및 조사를 위해서는 사용자의 요청을 처리하기 위한 클라우드 내 API 호출로 인해 생성되는 로그를 분석하는 것이 중요하다.

Table 1. Top 3 Cloud Threats

	Average Score	Issue Name
1	7.729927	Insufficient ID, Credential, Access and Key Mgt, Privileged Accounts
2	7.592701	Insecure Interfaces and APIs
3	7.424818	Misconfiguration and Inadequate Change Control

2.2 AWS CloudTrail

AWS CloudTrail은 AWS 환경에서 발생하는 API 호출을 기록하며, 보안 사고 발생 시 중요한 로그 정보를 제공하는 역할을 한다. 이를 통해 사용자가 언제, 어떤 서비스에 접근했는지, 영향받은 리소스는 무엇인지에 대한 파악과 공격자의 활동 등 사고와 관련된 중요 정보를 식별할 수 있다[9]. AWS Management Console, AWS SDK, AWS CLI 및 계정 활동에 대한 이벤트 기반 로깅을 지원하며 유형은 관리 이벤트, 데이터 이벤트, 인사이트 이벤트로 나뉜다[4]. 관리 이벤트는 AWS IAM (Identity and Access Management) 권한을 갖는 사용자 또는 역할로부터 자원과 서비스를 관리하거나 구성하는 작업, 예를 들어, EC2(Elastic Compute Cloud) 인스턴스와 S3(Simple Storage Service) 생성 등이 있다. 데이터 이벤트는 리소스와 리소스 내에서 수행된 작업을 기록하는 이벤트이다. 이는 S3 버킷에 저장된 파일이 삭제 및 수정되는 등 자원 내부 데이터 변경 또는 접근 관련 활동을 추적하는 데 유용하다. 이때, 데이터 이벤트는 기본적으로 비활성화되어 있으므로 사용자가 로그를 수집할 자원이나 유형을 추가해야 한다. 마지막으로 인사이트 이벤트는 비정상적인 활동에 대한 정보를 제공하는 것으로, API 사용량 변화가 일반적인 사용 패턴과 다를 때 로깅된다.

CloudTrail로 생성된 로그 데이터에서 확인할 수 있는 필드는 다양하다. API 호출이 이루어진 이벤트 날짜와 시간(UTC)을 나타내는 eventTime, 이벤트를 호출한 IAM의 자격증명을 확인할 수 있는 userIdentity, 요청이 이루어진 서비스를 알려주는 eventSource, 해당 서비스에 대한 API 요청 값 eventName, 요청이 이루어진 리전 awsRegion, 그리고 오류 정보를 확인할 수 있는 errorCode, errorMessage 등으로 구성된다[10]. 이중, eventName은 수행된 작업 유형을 식별할 수 있어 보안 모니터링 및 분석에 중요한 역할을 한다. 구체적으로, ‘ConsoleLogin’, ‘StartInstance’, ‘CreateUser’ 등의 eventName을 통해 로그인 이력, 서비스 활동 시간 외 접근한 자원 유형, 관리자 계정이 생성하지 않은 사용자 생성 등 특정 활동에 대한 API 호출 정보를 확인할 수 있다.

CloudTrail에 기록된 로그는 Fig. 1.과 같은 구조로 구성되어 있다. 해당 예시는 EC2 인스턴스 종

Fig. 1. TerminateInstances Event Log

료와 관련된 이벤트 로그의 일부분으로, 'TerminateInstances' 값을 가진 eventName을 확인할 수 있다. 특정 유형의 침해사고가 발생하였을 때 관련된 주요 필드와 데이터 유형을 빠르게 매핑시킬 수 있다면, 방대한 로그 중에서 불필요한 정보들을 빠르게 필터링하여 신속한 대응이 가능하다.

그러나 CloudTrail은 특정 침해사고와 관련된 주요 이벤트를 자동으로 식별하는 기능을 직접 제공하지 않는다. CloudTrail과 별도의 구독형 AWS 보안 솔루션인 Cloudwatch의 연동을 통해 모니터링이 가능하지만, 침해사고 대응 관점에서 사고 탐지 및 식별과 더불어 증거수집 및 분석을 위해서는 사용자가 로그를 직접 심층 분석해야 한다. 이 과정에서 많은 양의 로그 데이터를 직접 수동으로 분석해야 한다는 점과 침해사고 유형별로 어떠한 로그를 분석해야 하는지를 직접 판단해야 한다는 어려움이 존재한다. 본 논문에서는 다양한 필드 중에서도 사고 조사에 주요 필드로 판단되는 eventName을 기준으로 분석하여 이를 MITRE ATT&CK Matrix와 연계해 사고 조사에 활용하고자 한다. 구체적으로, 로그 데이터에서 발생하는 이벤트를 가시화해 분석할 수 있는 사고 탐지에 초점을 둔다. 이 과정에서는 모든 API 호출 정보를 포함한 관리 이벤트와 데이터 이벤트를 중심으로 다루며, 이를 통해 보안 위협을 식별하고 효과적인 대응 전략을 수립하는 데 필수적인 정보를 제공하고자 한다. 예를 들어, 적절한 권한이 없는 사용자의 비인가 접근 시도나, 구성 설정 오류로 인한 사고 등과 같은 상황에서 필요한 이벤트를 신속하게 식별할 수 있도록 효과적인 분류체계를 제안함으로써, 침해사고 대응 절차의 편의성과 신속성을 향상하고자 한다.

III. 관련 연구

클라우드 환경을 대상으로 한 위협이 증가함에 따라, 침해사고 대응을 위한 로그 분석 연구의 필요성 및 분석 방법론을 제안하는 연구들이 활발히 이루어지고 있다. Zaina AlSaed 외 2인은 클라우드 환경에서 포렌식 조사 시 직면하는 문제를 식별했다. IaaS(Infrastructure as a Service) 환경에서 클라우드 로그를 분석하는 과정에서 CSP(Cloud Service Provider)에 대한 의존성, 로그 수집과 무결성 문제, 클라우드 포렌식 도구의 부족함을 지적했다. 이러한 문제를 해결하기 위해 Apache Spark를 활용해 특정 기간 발생하는 대용량 로그 데이터 분석을 지원하는 포렌식 프레임워크를 구현했다. 그러나 이는 웹 서버 로그 데이터에 대한 포렌식 수행에 초점을 맞추었으며, 클라우드 환경에서 타임라인 재구성을 위한 로그 데이터 기반 시각화가 언급되었지만, 구체적인 구현은 제공되지 않았다[11].

Suleman Khan 외 7인은 CLF(Cloud Log Forensic)의 최신 기술을 검토하고 클라우드 로그 데이터 분석과 관련된 다양한 문제를 제시했다[12]. 그러나 분석을 위해 어떤 유형의 로그를 포함하고, 다양한 로그를 효과적으로 수집하고 분석할 방안에 대한 가이드라인을 제공하지 않았다. Kenny Awuson-David 외 4인은 클라우드 환경에서의 증거 획득을 위해 DSRM(Design Science Research Methodological) 접근 방법을 사용하여 BCFL(Blockchain Cloud Forensic Logging) 프레임워크를 제안하였다[13]. 그러나 블록체인과 같은 기술을 도입할 경우 분산 원장 유지와 트랜잭션 검증 등으로 인해 분석 프로세스가 더 복잡해질 수 있고, 클라우드 환경 성능과 효율성에 영향을 줄 수 있다.

클라우드 환경에서는 자원 생성이 간단하고 유동적인 서비스를 제공하기 때문에 대량의 로그 데이터가 생성된다. 클라우드 서비스의 API 호출 기반 운영 메커니즘은 데이터의 생성부터 저장 및 관리 과정

에서 기존 온프레미스 시스템의 한계를 넘어 다양하고 유연한 접근으로 변화시켰으며, API 호출에 따른 반응을 세밀하게 기록하여 더 많고 다양한 형태의 로그 데이터를 생성한다[14]. 클라우드 로그 데이터의 양과 다양성이 증가함에 따라, 침해사고 관점에서 이를 관리하고 분석하는 데 어려움이 존재한다. 본 연구에서는 선행연구에서 언급된 클라우드 로그 분석의 요구사항을 포함하여, 다양하고 방대하게 생성되는 데이터 중 침해사고 조사를 위한 로그들을 효율적으로 저장하고, 분석 및 분류할 수 있는 기준과 이를 자동화하여 관리해 주는 프레임워크를 개발하였다.

IV. Cloud Log Analysis Framework

4.1 프레임워크 개요

본 절에서는 AWS의 로깅 서비스인 CloudTrail로부터 수집된 로그를 기반으로 한 이벤트 분류체계 및 자동화된 로그 분석 프레임워크에 관하여 기술한다. 앞서 언급하였듯이, CloudTrail은 사용자 활동 및 API 호출을 통한 요청 매개변수, 시간, 이름 등 중요 정보를 기록한다. 이러한 정보는 CSP의 도움 없이 접근 가능하며, 데이터 암호화를 통해 무단 수정 및 읽기 방지로 무결성을 유지하므로 사고 조사에 있어 유용하다[15]. 이에 AWS 환경 내에서 로그 이벤트를 보다 정확하고 신속하게 분석하기 위해, CloudTrail 기반의 이벤트 분류체계를 활용한다.

현재 클라우드 환경에서 발생 가능한 위협은 크게 관리적 및 기술적 측면으로 분류되고 있지만[16], 이벤트를 기반으로 클라우드 환경에서 발생 가능한 위협을 분류하는 작업은 없다. 또한, 위협과 인스턴스 운용 과정에서 생성된 원시 로그 데이터 이벤트를 매핑하는 기준이 부족해 방대한 로그 분석의 진입점을 명확히 판단하는 데 어려움이 있다. 이에, 본 논문에서는 Cloud Matrix[17] 기반의 이벤트 분류체계를 제안하여 공격의 목적과 주요 이벤트를 신속히 식별하고자 한다[18]. MITRE가 제안한 ATT&CK(Adversarial Tactics, Techniques and Common Knowledge) Framework는 공격자의 행동과 수행 방식을 정의하며[9], 이는 신뢰할 수 있는 표준화된 체계 기반의 이벤트 로그 분류체계 구축에 기여한다[19]. 따라서, 발생한 사건에 대한 이해와 향후 발생 가능한 위협에 대응하는 능력을 향상할 수 있다.

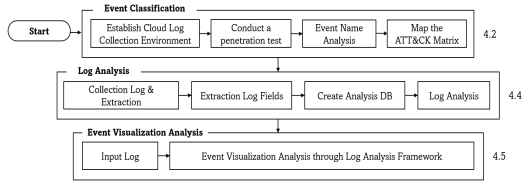

Fig. 2. Event Log Analysis Framework Overview

Fig. 2.는 제안하는 클라우드 로그 분석 프레임워크의 시스템 개요도 및 데이터 흐름을 나타낸다. 프레임워크는 크게 세 가지 모듈로 구성된다. 첫 번째는 ATT&CK Matrix 기반으로 이벤트를 식별하여 분류체계를 성립하기 위한 모듈이며, 두 번째는 사용자 행위 로그 데이터가 저장되는 모듈이다. 마지막은 두 모듈을 통한 분석 결과를 확인할 수 있는 시각화 분석 모듈이다.

4.2 이벤트 식별 모듈

4.2.1 클라우드 로그 수집환경 구축

본 절에서는 제안 프레임워크의 첫 수행 단계로 발생하는 이벤트의 eventName을 식별하기 위한 분석환경을 기술한다. 클라우드 환경에서의 로그는 시스템, 애플리케이션 및 네트워크 활동을 추적하고 모니터링하기 위해 다양한 소스에서 생성된다. 사용자(IAM), 네트워크, 애플리케이션 등 시스템 전체에서 발생하는 로그를 수집하는 데 필요한 일반적인 환경 구성은 Fig. 3.과 같다[20]. Amazon OpenSearch Service는 다양한 소스에서 발생하는 로그들을 모아 통합 분석이 가능하게 하며, 사용자 목적에 맞게 가시화해 주는 역할을 제공한다. 이는 발생한 이벤트를 실시간으로 확인하고 가시적으로 데이터를 분류하는 데 유용하다. 수집 경로는 CloudTrail을 통한 로그 수집이며, CloudTrail, CloudWatch, Lambda를 거쳐 OpenSearch로 로그 데이터가 수집되는 과정을 거친다. 이때 AWS에서는 자원에 대한 접근을 효과적으로 제어하기 위

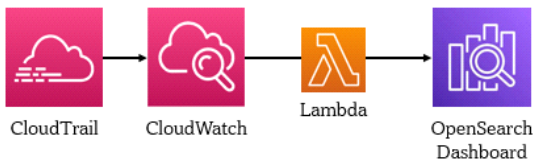

Fig. 3. Log collection/Analysis Environment

해 해당 자원 및 서비스에 대한 인증 및 권한을 부여해야 하는 경우가 많은데, 호출되는 Lambda에는 OpenSearch에 대한 권한이 있어야 로그 데이터 전송 및 통합이 가능하다[21]. 이러한 환경 구성을 통해 AWS 계정의 모든 API 호출 기록을 수집하고, 로그 이벤트를 통합 분석해 가시화할 수 있다.

4.2.2 침투 테스트 기반 위협 유형별 이벤트 로그 수집

클라우드 침해사고 유형별로 발생한 이벤트 로그를 수집하고 분류체계를 구성하기 위해, 침투 테스트 기반으로 클라우드 위협 발생을 발생시키고, 이때 생성된 이벤트 로그를 수집하는 작업을 선행하였다. Table 2.는 수행한 공격 행위의 일부로 Tactics에 따라 발생할 수 있는 이벤트를 나타낸다[22.23.24]. 이때, 침투 테스트를 위해 Stratus Red Team 오픈소스 프로젝트를 활용했다[23]. 이는 MITRE ATT&CK Framework에 기반하며, 클라우드 환경에서 일반적인 공격 기술을 시뮬레이션하는 데 중점을 둔 테스트 라이브러리이다. 이를 활용함으로써 다양한 Tactics를 기반으로 한 펜 테스트를 통해 이벤트 분석 기준을 마련할 수 있다.

또한, 제안한 프레임워크 환경에서 수집된 로그를 통합 관리하는 OpenSearch의 추가 기능을 활용하여 주요 이벤트 식별을 위한 지표로 활용하였다. 이를 통해, EC2 인스턴스 생성이나 콘솔 로그인과 같이 특정 이벤트 값의 급증을 감지하고 시간 범위를

Table 2. Events of the attack stage

Tactic	Event
Initial Access (TA0001)	Console Login without MFA
	Suspicious SAML Activity
Execution (TA0002)	Launch Unusual EC2 instances
	Change EC2 Startup Shell Script
Persistence (TA0003)	Create an Access Key on an existing IAM User
	Create a IAM User with administrative permissions
	Add a Malicious Lambda Extension
	Overwrite Lambda Function's Code

Fig. 4. Analysis Attack Time

필터링할 수 있다. Fig. 4.는 침투 테스트 후 OpenSearch에서 TSVB(Time Series Visual Builder)를 활용해 eventName에 대한 Count 값을 시각화한 것이다. TSVB는 로그 모니터링이나 특정 시간 동안의 활동을 가시화할 때 유용한 지표이다[21]. 각 Tactics 단계별로 발생 가능한 이벤트를 분석하기 위해 20시 47분에서 20시 53분 사이에 Persistence 단계의 침투 테스트를 실행했으며, 실제로 해당 시간 동안 특정 이벤트의 발생이 가장 빈번했음을 확인할 수 있다. 이처럼, 분석 시간대에 발생한 eventName을 중심으로 각 단계에 따른 이벤트를 분석 및 분류하는 작업을 진행했다. 이러한 지표는 침투 테스트뿐만 아니라 실제 사고 발생 시에도 특정 이벤트가 급증하거나 예상치 못한 시간에 발생한 이벤트를 식별하는 데 활용될 수 있다.

4.2.3 eventName 분석

eventName과 ATT&CK Matrix 매핑을 위해 앞서 언급한 침투 테스트 도구 및 공개된 룰 셋을 활용하고, Initial Access, Execution 등의 Tactics에 따라 세분화된 다양한 공격을 수행하여 로깅된 eventName을 분류하는 작업을 수행했다. 로그 이벤트 분류를 통해 공격 목표에 따른 침해사고 이벤트를 식별함으로써 체크리스트 기반의 로깅 검토 및 로깅 프레임워크를 설계할 수 있다. Fig. 5.와 Fig. 6.은 각각 Execution, Credential Access 단계의 테스트 수행 후 발생한 eventName을 CloudTag로 시각화한 결과를 나타낸 것이다. Fig. 5.의 Execution 단계 결과를 확인하면 EC2 인스턴스를 시작할 권한이 없는 IAM을 생성해 인스턴스를 실행하거나 악성 스크립트를 삽입한 후 관리자 권한으로 인스턴스가 실행되도록 하는 등의 이벤트 행위를 확인할 수 있다. 구체적으로 EC2 인스턴스의 속성을 관리하고 업데이트하는 'ModifyInstanceAttribute', 인스턴스의 종료 및 실행을 의미하는 'StopInstances', 'StartInstances'가 확인되었다. 이렇게 특정 공격을 발생시킨 시간을 기준으로 필터링한 후 로깅된 eventName을 확인

Fig. 5. Execution(TA0002) Events

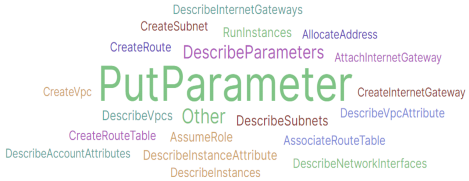

Fig. 6. Credential Access(TA0006) Events

함으로써 Matrix 매핑에 필요한 이벤트를 식별할 수 있다.

4.2.4 MITRE ATT&CK Matrix 매핑

이후 분류체계 구축을 위해 식별한 이벤트를 Cloud Matrix 기반으로 분류하였다. MITRE ATT&CK의 Cloud Matrix는 11개의 공격 기술과 행위를 설명하는 Tactics를 체계적으로 기술하고 있고, 각 Tactics를 달성하기 위한 공격 방법인 Techniques를 항목별로 분류해 제공한다[25]. 본 연구에서는 Tactics에 따른 eventName을 분류하였으며, 어떤 소스의 서비스로부터 발생한 이벤트인지 함께 매핑하여 데이터베이스화였다. 이를 통해, 침해사고 발생 시 서비스 기반 검색을 통해 사고 원인을 해석할 수 있다. 또한, eventName과 관련된 자원을 함께 분류함으로써 클라우드 자원 유형에 따른 조사 및 분석도 가능해진다. Table 3.은 ATT&CK Matrix와 eventName, 연결된 자원 및 서비스를 보여주는 분류체계의 일부이다. 이를 통해 호출된 API 정보가 어떤 공격과 Tactics, 자원 및 서비스와 관련 있는지 한눈에 파악하기 쉽다.

Table 3. Mapping ATT&CK Matrix

Event Name	Tactic	Technique	Service
Describe Task Definition	Persistence (TA0003)	Implant Internal Image (T1525)	ECS
Create User		Valid Accounts (T1078.004)	IAM
Create Access Key		Account Manipulation (T1098)	
List Buckets	Discovery (TA0007)	Cloud Infrastructure Discovery (T1580)	S3

4.3 eventName 통계 분석

본 절에서는 침투 테스트를 통해 수집된 483가지 eventName을 ATT&CK Matrix와 매핑한 통계 분석 결과를 기술한다. Fig. 7.은 Tactics 별 매핑된 eventName 수를 나타낸 것이다. 매핑 결과, Discovery(TA0007)와 Persistence(TA0003)가 높은 비율을 차지함을 식별하였다. 이는 침투 테스트 도구의 특성에서 비롯된 결과로 확인된다. Discovery(TA0007) 단계는 공격자가 시스템 내에서 수행 가능한 정보를 수집하는 활동에 해당하며, 침투 테스트 내 주요 행위 중 하나는 타겟 시스템의 서비스, 계정, 인프라 등 정보를 파악하기 위한 시뮬레이션을 수행한다. 타겟 시스템의 취약점을 식별하고 공격 범위를 확장하기 위해 다양한 정보를 수집하는 데 중점이 되는 펜 테스트 도구의 특징을 감안할 때, 해당 활동과 관련된 이벤트가 증가함은 도구의 목적과 부합함을 볼 수 있다.

다음으로 빈번하게 관찰된 Persistence 단계는 공격자가 시스템에 지속해 액세스를 유지하고 탐지를 피하기 위한 다양한 수단과 방법을 수행한다. 발생 가능한 이벤트 예시로는 백도어 설치, 계정 권한 상승 등이 있다. 침투 테스트는 시스템의 보안 강도를

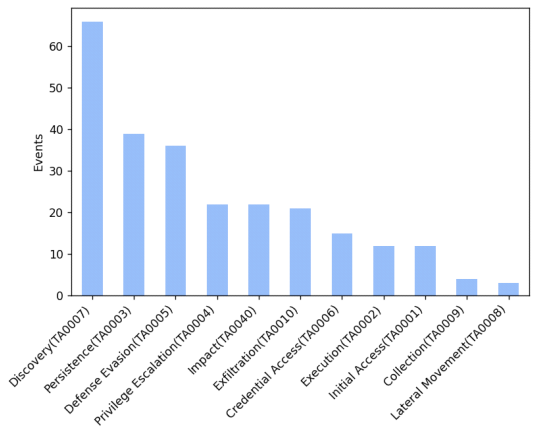

Fig. 7. eventName Analysis

확인하거나 잠재적인 취약점을 도출하기 위해 시스템에 의도적으로 침입하는 활동을 수행하며, 이 과정에서 흔히 사용되는 'Persistence' 기법을 시뮬레이션하거나 사용자의 권한을 상승시키는 등의 작업을 수행하기 때문이다.

Fig. 8.은 매핑된 eventName과 연관된 서비스의 발생 빈도이다. 분석 결과 EC2, IAM, S3 서비스 영역의 비중이 큰 것을 식별하였다. 이들은 AWS에서 핵심적이고 중요한 서비스들이며[26], 많은 애플리케이션과 시스템은 이러한 서비스들을 기반으로 운영되고 있다. 시뮬레이션된 환경도 주요 서비스에 대한 취약점 분석 및 공격을 수행하므로 해당 서비스들에 대한 로그 이벤트가 많이 발생한다. 또한, 이러한 결과는 Table 1.에서 보인 클라우드 침해사고 위협 분류 중 가장 빈번하게 발생한 위협 카테고리인 자원의 구성 관리 권한 오류와도 관련 있음을 보여준다.

Fig. 9.는 서비스와 Tactics 간의 매핑 결과를 히트맵으로 나타낸 것이다. 분석 결과에 따르면, Discovery(TA0007)-EC2, Discovery(TA0007)-S3가 가장 높은 빈도로 나타났음을 확인할 수 있다. Discovery(TA0007)는 공격자가 시스템 내에서 정보를 수집하는 활동을 나타내며, EC2와 S3는 AWS에서 핵심적이고 중요한 서비스이다. 따라서 이 히트맵 결과에서 두 서비스와 Discovery(TA0007)가 가장 빈번하게 연결되는 것은 시뮬레이션에서 주요 서비스를 활용한 정보 수집 활동이 주로 이루어졌음을 시사한다. 즉, 공격자가 시스템 내에서 EC2와 S3와 같은 주요 서비스에 접근하여 공격 수행을 위한 정보를 수집하고자 하는 시나리오가 빈번히 발생했음을 나타낸다.

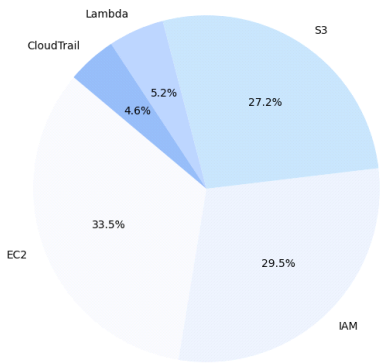

Fig. 8. Service Analysis

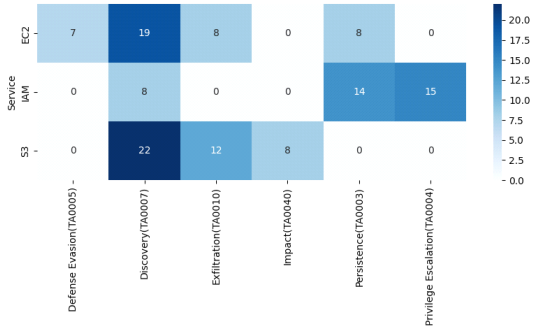

Fig. 9. Service-Tactics Analysis

이러한 통계 분석 결과는 보안 분석가에게 침투 테스트 도구를 통해 식별한 이벤트를 기반으로 실제 위협 활동 간의 상관성을 파악하는 데 유용한 인사이트를 제공할 것이다. 이때, 본 연구에서 활용한 Stratus Red Team 외에 추가적인 침투 테스트 도구를 바탕으로 매핑 작업을 업데이트할수록 Tactics에 따른 다양한 eventName 분석 커버리지가 증가할 것이다.

4.4 로그 저장 및 분석 모듈

본 절에서는 4.2에서 ATT&CK Matrix를 기반으로 분류된 이벤트를 실제 행위 로그와 연계 분석하기 위해 필요한 로그 저장 및 분석 모듈에 관해 설명한다. 해당 모듈의 주요 기능은 로그 수집 및 추출, 분석을 위한 로그 필드 선정, 데이터베이스화로 구성된다.

4.4.1 로그 수집 및 추출 & 필드 추출

로그 분석 모듈의 첫 수행 단계는 분석할 사용자 로그 데이터 내 주요 필드를 추출하는 과정이다. CloudTrail은 AWS 자원에 대한 변경 및 액세스 이벤트를 Amazon S3로 저장할 수 있으며, 이를 CSV나 JSON 형식으로 추출할 수 있다. 본 연구에서는 유연성과 확장성을 고려해 JSON 데이터를 분석하고 이를 데이터베이스에 저장한다. 이때, 행위 분석을 위한 로그 필드를 파악해야 한다. 제안된 프레임워크의 필드 분석에서는 저장 효율성을 고려하여 모든 로그 필드가 아닌 4W1H(Who, When, Where, What, How)를 기준으로 정보를 추출해 행위 분석 시 "누가, 언제, 어디서, 무엇을, 어떻게"의 최소 이벤트 표현이 가능하게 한다. 이러한 접근

을 통해 로그 데이터의 저장을 효율적으로 할 수 있다. Table 4.의 첫 번째 열은 AWS CloudTrail에서 해당 기준으로 추출한 필드를 보여준다.

기본적으로는 경량성을 갖춘 DB를 생성하기 위해 로그 필드를 선별하였지만, 때에 따라 심층 분석 시 원본 로그 전체 정보가 있어야 하는 경우가 존재한다. 이를 위해 이벤트의 고유 식별자를 나타내는 eventID 필드를 추가하여 로그 데이터의 실제 저장 위치를 확인할 수 있도록 했다. 이에 모든 필드가 DB에 적재되지 않더라도 eventID를 통해 원본 로그에 접근할 수 있다.

Table 4. Log Table Fields / OCSF

	AWS	Description	OCSF
Who	user Identity	User information (user identifier, name, MFA authentication etc.)	unmapped {userIdentity.~}
When	event Time	Time of event occurrence	time
Where	event Source	Source or type of the event	service.name
	source IP Address	IP address from which the request was made	src_endpoint.ip
	aws Region	Region where the event occurred	cloud.region
What	event Name	Name of the event	operation
	request Parameters	Parameters of the API request performed in the respective event	unmapped.{requestParameters.~}
How	user Agent	Agent from which the request was made	http_request.user_agent
	error Code	Error code (If the request returns an error)	api.response.error
	error Message	Error description	api.response.message
ID	eventID	Event identifier	-

그러나 AWS CloudTrail 필드에 기반한 추출을 통해서는 다양한 클라우드 침해사고 유형을 통합하여 표준화된 형태로 관리하는 것이 불가능하다. 이는 클라우드 플랫폼의 로그는 형식과 스키마가 다르기 때문이며, AWS를 포함하여 Microsoft Azure, Google Cloud Platform(GCP) 등 대표적인 클라우드 플랫폼별로 로그 데이터의 관리 방법은 차이가 있다. 실제로 ELK Stack 기반으로 AWS와 Azure에서 발생한 로그를 수집하고 분석한 결과, 로그 데이터가 정규화되지 않고 각 클라우드 환경에서 발생한 로그 형식으로 수집됨을 확인하였다. 이는 로그를 통합 수집하는 환경을 구축하더라도, 이종의 환경에서 발생하는 로그 유형 및 포맷이 다르므로 효과적인 사고 분석이 어렵다는 것을 보여준다. 따라서 플랫폼 간 로그 필드 명칭을 표준화하고 일관된 형식을 적용하는 것이 중요하다.

이에 본 연구에서는 개방형 사이버 보안 프레임워크인 OCSF(Open Cybersecurity Schema Framework)를 기준으로 하여, CloudTrail에서 분석된 로그 필드와 동일한 OCSF의 필드 매칭을 수행하였다. 이를 통해, 특정 벤더에 제약 사항이 없는(vendor-agnostic) 분류법을 제공하여 이종의 클라우드 환경에 대한 정규화 작업 없이 데이터 수집 및 분석을 향상할 수 있도록 지원한다[27]. 예를 들어, Table 4.와 같이 CloudTrail의 eventName은 OCSF 상에서 operation, event Time은 time의 형태로 정의됨을 식별하였다. 로그 분석 시 이러한 정규화 표준 체계가 적극적으로 수립된다면, 다양한 클라우드 플랫폼에서의 통합 분석 시 데이터 정규화에 드는 시간과 노력을 절약할 수 있다.

4.4.2 로그 분석 데이터베이스 생성

로그 저장 및 분석 모듈의 또 다른 주요 기능은 분석된 정보를 데이터베이스화하는 것이다. DB 구성 시 FK(Foreign Key)를 통한 테이블 간의 연결을 설정함으로써, 행위 관련 정보를 효과적으로 통합할 수 있다. Fig. 10.은 구성한 DB의 스키마이고, Fig. 11.과 Fig. 12.는 정의한 스키마의 테이블에 대한 세부 정보이다. log 테이블에는 Table 4.에서 추출한 로그 필드의 데이터가, eventName_attck 테이블에는 eventName에 매칭되는 Tactics와

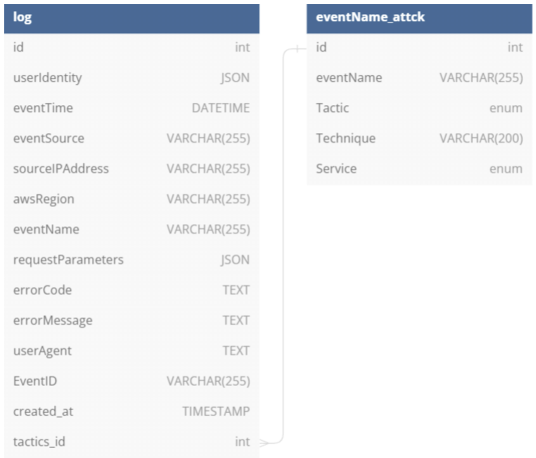

Fig. 10. DB Schema

id	userIdentity	eventTime	eventSource	sourceIPAddress	awsRegion	eventName	requestParameters	errorCode	errorMessage	userAgent	EventID	created_at	tactics_id
25	{"arn": "arn...	2023-12...	s3.amazona...	210.125.93.124	us-east-1	ListObjects	{"Host": "s3.amazo...	NULL	NULL	[S3Consol...	fce76a...	2023-12-2...	450
26	{"type": "A...	2023-12...	s3.amazona...	cloudtrail.amaz...	us-east-1	PutObject	{"key": "AWSLogs/...	NULL	NULL	cloudtrail....	061e6c...	2023-12-2...	439
27	{"arn": "arn...	2023-12...	s3.amazona...	210.125.93.124	us-east-1	ListObjects	{"Host": "s3.amazo...	NULL	NULL	[S3Consol...	2a8b4e...	2023-12-2...	450
28	{"type": "A...	2023-12...	kms.amazon...	cloudtrail.amaz...	us-east-1	GenerateD...	{"keyId": "arn:aws:...	NULL	NULL	cloudtrail....	f091eb...	2023-12-2...	411
29	{"arn": "arn...	2023-12...	cloudtrail.a...	210.125.93.124	us-east-1	LookupEvents	{"maxResults": 50, ...	NULL	NULL	Mozilla/5.0...	20d347...	2023-12-2...	220
30	{"arn": "arn...	2023-12...	health.amaz...	210.125.93.124	us-east-1	DescribeEv...	{"filter": {"startTim...	NULL	NULL	AWS Inter...	ea1772...	2023-12-2...	451
31	{"arn": "arn...	2023-12...	s3.amazona...	210.125.93.124	us-east-1	ListBuckets	{"Host": "s3.amazo...	NULL	NULL	[S3Consol...	1243fd...	2023-12-2...	136
32	{"arn": "arn...	2023-12...	ec2.amazon...	210.125.93.124	us-east-1	DescribeRe...	{"regionSet": {}, "a...	NULL	NULL	Mozilla/5.0...	18abf5...	2023-12-2...	200

Fig. 11. log Table

id	eventName	Tactic	Technique	Service
4	ConsoleLogin	Initial Access(TA0001)	Valid Accounts(T1078)	IAM
470	UpdateSAMLProvider	Initial Access(TA0001)	Valid Accounts(T1078)	IAM
471	UpdateSAMLProvider	Defense Evasion(TA0005)	Use Alternate Authentication Material(T1550)	IAM
473	AssumeRoleWithSAML	Initial Access(TA0001)	Valid Accounts(T1078)	STS
474	AssumeRoleWithSAML	Defense Evasion(TA0005)	Use Alternate Authentication Material(T1550)	STS

Fig. 12. eventName_attck Table

Techniques, 서비스 정보가 각각 저장된다. 이때, ATT&CK Matrix를 기반으로 한 이벤트 정보를 제공함으로써 다양한 공격 기술 및 전술에 대한 정보를 로그와 통합 분석한다. 이를 통해 행동 패턴의 위험성을 식별하고, 공격에 대한 종합적이고 심층적인 분석을 통해 효과적인 사고 조사가 가능하며, 로그 자체로는 파악하기 어려운 정보를 얻을 수 있다.

4.5 시각화 분석 모듈

침해사고를 위한 로그 분석을 위해서는 클라우드 환경에서 발생한 이벤트를 직관적으로 파악하고, 다양한 로그 데이터에서 조사할 주요 이벤트를 빠르게 식별하기 위한 시각화가 중요하다. 따라서, 제안한 프레임워크는 이벤트 식별 및 로그 분석 모듈을 가시화하여 사용자가 직관적으로 이벤트 분포를 이해하고 효과적으로 분석하기 위해 GUI 형태의 대시보드를 제공한다. Fig. 13.은 직접 구현한 ATT&CK Matrix-eventName 기반 로그 분석 프레임워크의 GUI 화면이다. Tkinter를 이용하여 구현된 GUI는 사용자에게 직관적이고 사용하기 편리한 환경을 제공한다. 이는 Python의 표준 GUI 라이브러리로, 간편한 사용과 다양한 GUI 응용 프로그램을 개발할 수 있는 효과적인 도구로 널리 사용되고 있다[28]. 또한, Matplotlib과 Seaborn을 활용한 히트맵은 이벤트와 Tactics에 대한 빈도를 직관적으로 시각화하여 사용자에게 효과적인 이벤트 분석 도구를 제공한다.

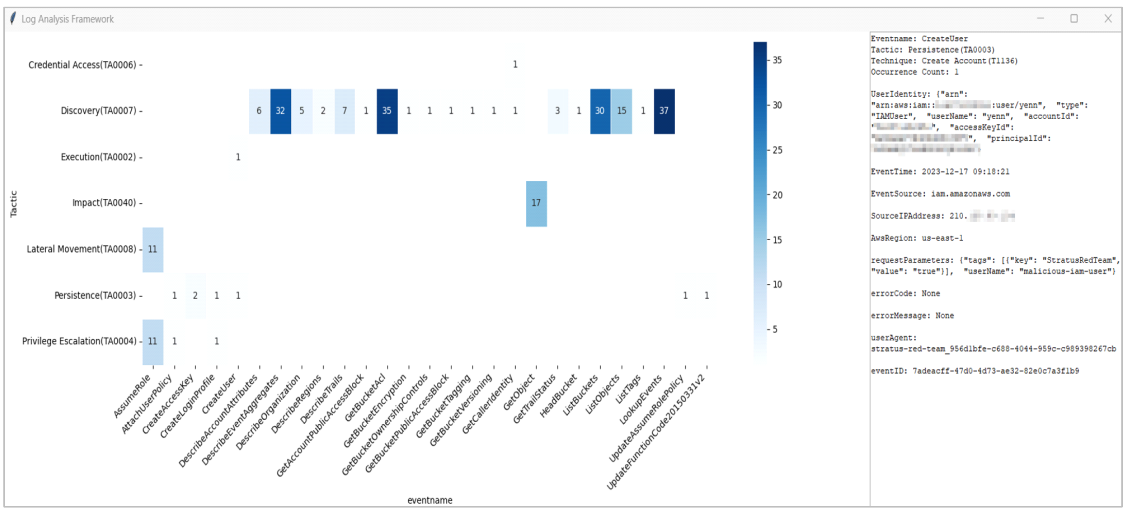

Fig. 13. Automated Log Analysis Framework GUI

프레임워크 실행 시, x축에는 발생한 이벤트가 표시되며 y축에는 이벤트에 대응하는 Tactics가 나타난다. 두 축의 정보를 분석하여 이벤트의 발생 빈도를 정량적으로 파악할 수 있으며, 특정 이벤트에 대한 상세 정보를 탐색하기 위해 셀을 선택할 수 있다. 선택된 셀에 대한 분석을 진행할 때, 사용자 인터페이스의 우측 부분에는 해당 이벤트 로그의 상세 정보를 확인할 수 있는 영역이 제공된다. 이 영역에서는 해당 이벤트의 Tactics과 Techniques 정보를 확인할 수 있다.

V. 성능 평가

본 절에서는 제안한 프레임워크의 활용 가치를 입증하기 위해 침해사고 유형별 시나리오에서 생성된 이벤트 로그를 분석하고, 분류된 이벤트와의 매칭 결과를 비교하여 평가를 수행한다.

5.1 ATT&CK Tactics 커버리지 분석

로그 분석 프레임워크는 ATT&CK Matrix를 기반으로 하였기 때문에, 각 Tactics에 대응하는 eventName의 정확한 식별이 가능한지에 대해 평가했다. 이를 위해 ATT&CK Framework와 연계된 테스트 라이브러리를 활용해 실험 환경을 구축하고, 생성된 로그 데이터를 기반으로 커버리지를 분석했다[22.23.29]. 이는 클라우드 환경에서 위협 공격을 시뮬레이션할 수 있는 실질적인 메커니즘을 제공한다. 평가 핵심은 각 Tactics에 대응하는 eventName을 얼마나 정확하게 감지하고 분류하는지를 통해, 프레임워크가 주요 이벤트를 식별하고 판단하는 데 실효성을 갖추고 있는지 검증한다. 평가를 위해 이벤트 분석 결과에서 가장 큰 비중을 차지한 Discovery(TA0007)와 Persistence(TA0003) 단계의 커버리지 테스트를 수행했다. 또한, Credential Access(TA0006) 단계는 공격자가 피해자의 인증 정보를 확보해 시스템이나 네트워크의 접근 및 권한을 얻을 수 있게 하는 중요한 단계임을 고려하여, 실험 과정에 해당 단계도 수행하였다.

5.1.1 Discovery(TA0007) 분석

Table 5.는 침투 단계 중 Discovery(TA0007)에 해당하는 공격 활동을 설명한다. 이는 주로 공격자가

Table 5. Discovery Attack techniques

Technique	Description	Detection
ec2-enumerate-from-instance	Execute the scan command	Detect instances of abnormal enumeration calls(e.g., ListBuckets)

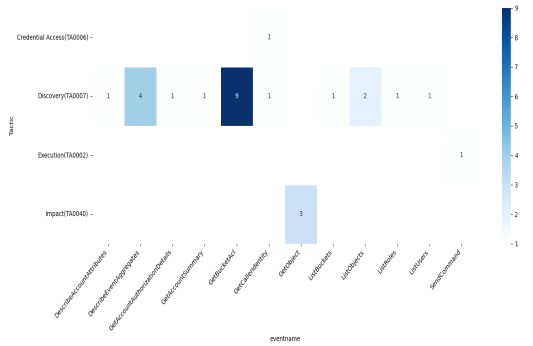

Fig. 14. Discovery Heatmap

수행하는 초기 정보 수집 및 탐색에 해당하며, 본 침투 테스트에서는 손상된 EC2에서 공격을 위한 정보를 탐색한다. Fig. 14.는 공격자가 환경을 탐색하고 정보를 수집하기 위해 수행한 활동 로그를 분석 프레임워크를 통해 시각적으로 나타낸 것이다. 분석 결과, 사용자 또는 역할에 대한 정보를 검색하여 호출자의 계정 ID 및 IAM 구성을 확인할 수 있는 'GetCallerIdentity'와 'GetAccountSummary', AWS S3 버킷의 목록을 가져오는 'ListBuckets', 계정 내의 모든 IAM 역할과 사용자를 확인할 수 있는 'ListRoles'와 'ListUsers', IAM 객체에 대한 자세한 권한 정보를 확인하는 'GetAccountAuthorizationDetails' 등 공격자가 환경을 탐색하고 정보를 수집하는 단계를 수행하기 위한 Discovery 연관 이벤트가 직관적으로 식별되는 것을 볼 수 있다.

5.1.2 Persistence(TA0003) 분석

Table 6.은 Persistence(TA0003) 단계에서의 공격 기술을 나타낸다. 이는 공격자가 시스템에 지속적인 액세스를 확보하기 위한 단계로, 접근 권한을 유지하기 위해 기술 및 행위를 수행한다. Fig. 15.는 공격자가 지속적인 액세스를 유지하기 위해 행한 이벤트를 제안한 프레임워크를 통해 시각적으로 분석한 것이다. 악의적인 사용자가 IAM 역할에 백도어를 추가하는 과정에

Table 6. Persistence Attack techniques

Technique	Description	Detection
iam-back door-role	Add a backdoor to an IAM role	Detect 'UpdateAssume RolePolicy' event
iam-back door-user	Add an access key to an existing IAM user	Detect 'CreateAccess Key' event
iam-create-admin-user	Create a new IAM user(root)	Detect 'CreateUser', 'AttachUserPolicy' and 'CreateAccessKey' events
iam-create-user-login-profile	Create a profile on an existing IAM user	Detect 'CreateLogin Profile' or 'UpdateLogin Profile' event
lambda-over write-code	Overwrite a Lambda function's code	Detect 'Update Function Code~' event

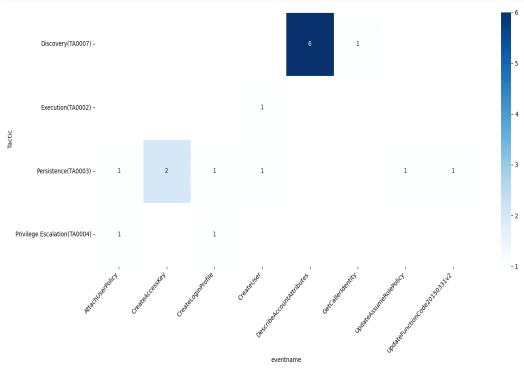

Fig. 15. Persistence Heatmap

서 'UpdateAssumeRolePolicy', 기존 IAM 사용자에게 액세스 키를 추가하는 'CreateAccessKey', 루트 권한을 갖는 새로운 IAM 사용자를 생성하는 'CreateUser', 'AttachUserPolicy', 'CreateAccessKey', 기존 IAM 사용자에게 프로파일을 생성하는 'CreateLoginProfile', 'UpdateLoginProfile', 람다 함수의 코드를 덮어쓰는 'UpdateFunctionCode~*' 등 계정의 유효성 및 지속성을 확립하기 위해 수행하는 Persistence 관련 이벤트가 직관적으로 분석된 것을 확인할 수 있다.

5.1.3 Credential Access(TA0006) 분석

Table 7.은 Credential Access에 해당하는 공격 기술을 수행한 설명으로, 각 단계에서의 공격 기술과 탐지를 위한 주요 eventName을 확인할 수 있다. Credential Access 단계는 공격자가 시스템 내에서 유효 자격을 획득하려는 단계로, EC2 인스턴스 내 RDP(Remote Desktop Protocol) 암호 탈취를 시도하거나 자격증명 검색과 같은 다양한 기술과 기법을 통해 시스템에 로그인할 수 있는 권한을 획득하려고 한다. Fig. 16.은 실제 다양한 기법을 수행한 공격 로그를 분석 프레임워크로 실행한 결과를 나타낸다. 실제로 암호화된 관리자 비밀번호를 검색하는 'GetPasswordData', IAM 사용자 또는 역할에 대한 세부 정보를 반환하는 'GetCallerIdentity', 인스턴스의 정보를 출력하는 'DescribeInstances' 등 Credential Access 단계에서의 주요 이벤트가 다뤄진 것을 시각적으로 확인할 수 있다.

만일 공격자가 클라우드 환경에서 권한을 획득할 경우(서비스를 손상해 높은 권한의 계정 자격 증명

Table 7. Credential Access Attack techniques

Technique	Description	Detection
ec2-get-password-data	Steal RDP credentials within a running EC2 instance	Identify the entity with a high frequency of 'GetPasswordData' events
ec2-steal-instance credentials	Unauthorized acquisition of EC2 instance credentials from the Instance Metadata Service	Identify the entity that attempted to call 'GetCallerIdentity'
secretsmanager retrieve-secrets	Search for passwords stored in Secrets Manager	Identify the subject that searches for the password and detect 'ListSecrets', 'GetSecretValue' events
ssm-retrieve-securestring-parameters	Generate a large number of Systems Manager parameters available in AWS regions	Identify that retrieves large numbers of SSM parameters and detect 'GetParameters' events

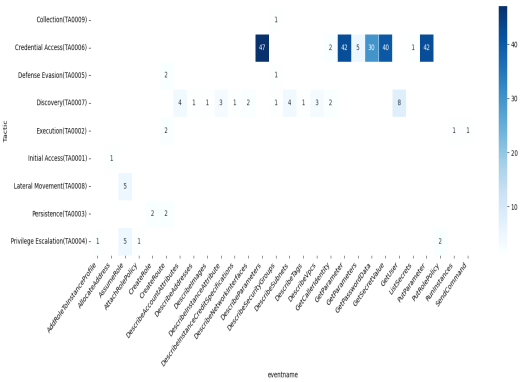

Fig. 16. Credential Access Heatmap

획득) 관리자에게 비밀 정보를 요청할 수 있다[30]. 이러한 유형의 공격(Table 7.의 secretsmanager-retrieve-secrets)을 탐지하기 위해서는 CloudTrail의 'GetSecretValue' 이벤트를 발생시켜 많은 수의 비밀 정보를 검색하는 주체를 식별해야 한다. 이때, 분석 프레임워크의 셀 선택 기능을 활용하면 'GetSecretValue' 이벤트에 대한 상세 정보 확인이 가능하다. 예를 들어, Fig. 17.과 같이 해당 이벤트

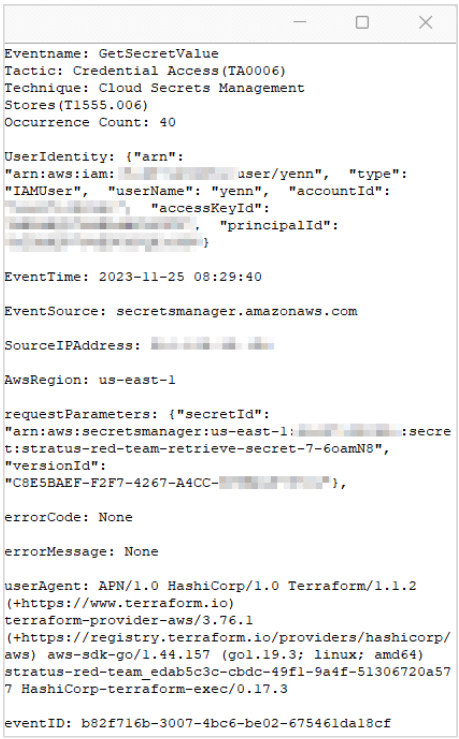

Fig. 17. Selected Event Cell

의 발생 빈도, 시간, ATT&CK Techniques, 호출한 사용자 식별 정보 등을 확인할 수 있다. 이를 통해 대량의 로그 파일 중 분석해야 할 이벤트를 직관적으로 선택하고, 관련 로그를 분석할 수 있다.

이처럼, 제안한 이벤트의 시각적 분석 프레임워크는 대량의 로그 파일에서도 신속한 분석 및 이벤트 판단이 가능함을 다양한 사례 연구를 통해 확인하였다. 이를 통해 대규모의 데이터를 효과적으로 해석하고, 보안 이슈를 신속하게 감지하고 대응할 수 있을 것으로 기대한다.

VI. 결 론

클라우드 컴퓨팅 환경은 대량의 로그 데이터가 생성되기 때문에 이벤트를 분류체계에 따라 정의하고, 이를 효과적으로 분석하는 것은 중요하다. 본 논문에서는 AWS 환경에서의 사고 조사를 위해 CloudTrail을 통한 이벤트 로그를 수집하고, 이를 ATT&CK Matrix와 연계하여 분석할 수 있는 이벤트 시각화 분석 프레임워크를 제안했다. 이를 통해 침해사고 발생 시 필요한 로그 이벤트를 신속하게 식별해 효율적인 로그 분석을 수행할 수 있다. 제안한 프레임워크는 사고 조사 관점에서 다음과 같은 이점을 제공한다.

첫 번째로, 사고 발생 시 매핑된 정보를 기반으로 방대한 로그 데이터 중 어떤 유형의 이벤트를 추적해야 하는지 신속하게 판단할 수 있다. 분석 프레임워크를 활용하면 AWS CloudTrail에서 수집된 데이터를 체계적으로 분석하여 시스템 이벤트를 자동으로 식별할 수 있다. 시각적인 표현은 이러한 분석 결과를 직관적으로 파악할 수 있게 도와주며, 클라우드 환경에서 발생하는 다양한 위협에 대한 이벤트를 신속하게 파악할 수 있게 된다. 이를 통해 로그 분석에 소요되는 시간과 노력을 줄일 수 있다. 두 번째로, 주요 eventName을 선별해 사건의 경과와 원인을 파악할 수 있고, 이는 사건 재구성을 가능하게 한다. eventName은 어떤 단계나 행동이 수행되었는지를 추적하는 데 도움 되므로 AWS 환경에서의 공격자 경로를 빠르게 식별할 수 있다. 또한, 이벤트와 ATT&CK Matrix 간의 연계를 활용해 특정 사고와 관련된 이벤트 패턴을 식별하고, 이를 기반으로 수사 전략을 수립할 수 있다. 세 번째로, CloudWatch의 임곗값을 설정하기 위해 특정 트리거 포인트를 분석하고 적용하는 플러그인 기반 접근

방식으로 활용할 수 있다. 이를 통해, 특정 이벤트가 발생했을 때 세부적인 경고를 설정할 수 있으며, 이는 위협을 보다 명확하고 효율적으로 식별하는 데 도움이 된다.

현재 클라우드 환경에서 로그 이벤트를 분석하기 위한 적절한 가이드라인 연구가 부족한 상황에서, 제안한 프레임워크는 효과적인 사고 조사 프로세스를 구축하는 데 기여한다. 클라우드 컴퓨팅 환경의 로그 데이터를 활용해 행위를 분석하는 연구는 지속해서 요구되며, 이를 통해 증가하는 클라우드 보안 위협 사례에 대응하고, 조사하는 방안을 모색하는 것이 중요하다. 향후 연구에서는 제안된 프레임워크의 시스템 효율성을 높이기 위해 메모리 저장 효율성을 포함해 성능을 개선하는 프로세스 구현과 이상 탐지 기능 향상에 중점을 둘 것이다. 또한, AWS 환경에만 국한되지 않고 Azure, GCP 등 다양한 클라우드 플랫폼으로의 확장을 고려해 환경에 제약되지 않는 로그 이벤트의 정규화 스키마를 적용하고자 한다.

References

[1] "Gartner, Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 Billion in 2023", Gartner, Apr. 19, 2023.

[2] James Guffey and Yanyan Li, "Cloud Service Misconfigurations: Emerging Threats, Enterprise Data Breaches and Solutions", 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), pp. 806-812, Mar. 2023.

[3] Pranitha Sanda, Digambar Pawar, and V. Radha, "An insight into cloud forensic readiness by leading cloud service providers", Computing, vol. 104, no. 9, pp. 1-26, Apr. 2022.

[4] AWS, What is AWS CloudTrail?, "CloudTrail", https://docs.aws.amazon.com/ko_kr/awscloudtrail/latest/userguide/cloudtrail-user-guide.html, Sep. 23, 2023.

[5] Microsoft, Azure Monitor activity log, "Activity log", https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log?tabs=powershell, Oct. 3, 2023.

[6] AWS, What is Amazon CloudWatch?, "CloudWatch", https://docs.aws.amazon.com/ko_kr/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html, Sep. 23, 2023.

[7] Hussain Akbar, Muhammad Zubair and Muhammad Shairoze Malik, "Security Issues and challenges in Cloud Computing", International Journal for Electronic Crime Investigation, vol. 7, no. 1, pp. 13-32, Mar. 2023.

[8] Jon-Michael Brook, Alexander Stone Getsin, and Michael Roza, "Top Threats to Cloud Computing: Pandemic 11 Deep Dive", Cloud Security Alliance (CSA), Oct. 2023.

[9] Simeen Sheikh, Ganesan Suganya, and Premalatha Mariappan, "Automated Resource Management on AWS Cloud Platform", Proceedings of 6th International Conference on Big Data and Cloud Computing Challenges : ICBCC 2019, pp. 133-147. Oct. 2019.

[10] AWS, CloudTrail record contents, "CloudTrail record", https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference-record-contents.html, Sep. 23, 2023.

[11] Z. AlSaed, M. Jazzar, A. Eleyan, T. Bejaoui, and S. Popoola, "An Integrated Framework Implementation For Cloud Forensics Investigation Using Logging Tool", 2022 International Conference on Smart Applications, Communications and Networking, pp. 1-6, Dec. 2022.

[12] Suleman Khan, Abdullah Gani, Ainuddin Wahid Abdul Wahab, Mustapha Aminu Bagiwa, Muhammad Shiraz, Samee U. Khan, Rajkumar Buyya, and Albert Y. Zomaya, "Cloud

Log Forensics: Foundations, State of the Art, and Future Directions", ACM Computing Surveys, vol. 49, no. 1, pp 1 - 42, May. 2016.

[13] Kenny Awuson-David, Tawfik Al-Hadhrami, Mamoun Alazab, Nazaraf Shah and Andrii Shalaginov, "BCFL logging: An approach to acquire and preserve admissible digital forensics evidence in cloud ecosystem", Future Generation Computer Systems, vol. 122, no. 2, pp. 1 - 13, Sep. 2021.

[14] Ju Young Kim and Soon-Hee Kim, "A Study on Transferring Electronic Records from Record Production System to Record Management System Using Cloud Storage". Journal of Korean Society of Archives and Records Management, 19(2). pp. 1-24. May.2019.

[15] Benjamin Yankson and Adam Davis, "Analysis of the Current State of Cloud Forensics: The Evolving Nature of Digital Forensics", 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), pp. 1-8, Nov. 2019.

[16] Top Cloud Security Challenges in 2023, "Cloud Security", https://orca.security/resources/blog/the-top-5-cloud-security-risks-of-2023/, April. 14, 2023.

[17] MITRE ATT&CK, "Cloud Matrix", https://attack.mitre.org/matrices/enterprise/cloud/, Dec. 21, 2023.

[18] Chanho Shin and Changhee Choi, "Cyberattack Goal Classification Based on MITRE ATT&CK: CIA Labeling", Journal of Internet Computing and Services(JICS), 23(6), pp. 15-26, Dec. 2022.

[19] P Rajesh, Mansoor Alam, Mansour Tahernezhadi, A Monika, and Gm Chanakya, "Analysis Of Cyber Threat Detection And Emulation Using MITRE Attack Framework", 2022 International Conference on Intelligent Data Science Technologies and Applications(IDSTA), pp. 4 - 12, Sep. 2022.

[20] AWS. Building a SIEM with AWS services, "SIEM", https://catalog.us-east-1.prod.workshops.aws/workshops/2ff04db5-bb02-4208-b637-d54a352f7bc6/ko-KR/10-siem, Sep. 23, 2023.

[21] Chen Qian, Yan Wang, and Lei Guo, "A novel method based on data visual autoencoding for time-series classification", Proceedings of the 2015 Chinese Intelligent Automation Conference, Lecture Notes in Electrical Engineering, pp. 97-104, Mar. 2015.

[22] Stratus Red Team, "Stratus", https://stratus-red-team.cloud/, Dec. 23, 2023.

[23] DataDog, stratus-red-team, "Stratus", https://github.com/DataDog/stratus-red-team/tree/main, Dec. 23, 2023.

[24] SigmaHQ. Sigma, "Sigma", https://github.com/SigmaHQ/sigma, Dec. 23, 2023.

[25] Chan-Woong Hwang, Sung-Ho Bae, and Tae-Jin Lee, "MITRE ATT&CK and Anomaly detection based abnormal attack detection technology research", Journal of Information and Security, 21(3), pp. 13-23, Sep. 2021.

[26] Shilin He, Qingwei Lin, Jian-Guang Lou, Hongyu Zhang, Michael R. Lyu, and Dongmei Zhang, "Identifying impactful service system problems via log analysis", Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, pp. 60 - 70, Oct. 2018.

[27] Paul Agbabian, "Understanding the

Open Cybersecurity Schema Framework(OCSF)", Aug. 2023.
〔28〕 Alan D Moore, Python GUI Programming with Tkinter: Design and build functional and user-friendly GUI applications, Packt Publishing Ltd, Mar. 2022.
〔29〕 Alexander M. Kirksharian, "Solving the Skills Gap: A Dynamic Approach to Cybersecurity Training", M.S. Thesis, San Diego State University, Dec. 28, 2023.
〔30〕 MITRE ATT&CK, Credentials from Password Stores: Cloud Secrets Management Stores, "Password Managers", https://attack.mitre.org/techniques/T1555/006/, Dec. 31, 2023.

〈저자소개〉

김 예 은 (Yeeun Kim) 학생회원
2022년 8월: 성신여자대학교 융합보안공학과 학사
2024년 2월:성신여자대학교 미래융합기술공학과 석사
〈관심분야〉 정보보호, 클라우드 컴퓨팅, 디지털 포렌식

김 정 아 (Junga Kim) 학생회원
2020년 3월~현재: 성신여자대학교 융합보안공학과 학사
〈관심분야〉 클라우드 컴퓨팅, 디지털 포렌식

채 시 윤 (Siyun Chae) 학생회원
2020년 3월~현재: 성신여자대학교 융합보안공학과 학사
〈관심분야〉 클라우드 컴퓨팅, 디지털 포렌식

홍 지 원 (Jiwon Hong) 학생회원
2021년 3월~현재: 성신여자대학교 융합보안공학과 학사
〈관심분야〉 클라우드 컴퓨팅, 디지털 포렌식

김 성 민 (Seongmin Kim) 종신회원
2012년 2월: 한국과학기술원 전기 및 전자공학과 졸업
2014년 2월: 한국과학기술원 전기 및 전자공학과 석사
2019년 2월: 한국과학기술원 정보보호대학원 박사
2019년 9월~2020년 8월: 삼성전자 삼성리서치 Staff Engineer
2020년 9월~현재: 성신여자대학교 융합보안공학과 조교수
〈관심분야〉 신뢰 실행 환경, 클라우드 컴퓨팅, 시스템 보안