SaaS 기업 대상 CSAP 대응 쿠버네티스 환경 보안 진단 및 상용 LLM 보고서 자동화 시스템

박도윤*, 이형규*, 임윤태*, 이재환*

*네이버 클라우드 캠프, *이스트소프트

*doyunpark93@gmail.com, *itisaknife234@gmail.com, *yimyuntae2000@gmail.com,
*dolchi37@gmail.com

CSAP Response System for SaaS Companies Kubernetes-Based Security Assessment and Automated Reporting with Commercial LLMs

Do-Yun Park*, Hyeong-Gyu Lee*, Yun-Tae Yim*, Jae-Hwan Lee*

*NAVER CLOUD CAMP, *EST SOFT.

요 약

최근 빠른 정보통신기술과 5G 기술의 발전은 클라우드 컴퓨팅 기술의 본격적인 확산으로 이어졌다. 특히 중소 규모의 기업들도 컨테이너 기반의 클라우드 네이티브 환경을 채택하면서 이를 관리하는 쿠버네티스가 핵심 인프라로 자리 잡았다. 이러한 환경은 SaaS 형태로 서비스 제공이 이루어져, CSAP와 같은 보안 인증 요구를 통해 보안을 강화하였다. 하지만 빠른 배포와 자동화를 지향하는 환경에서는 보안 검증이 미흡해질 수 있으며, 이에 따라 클러스터 보안 위협 대응에 대한 필요성이 커지고 있다. 본 연구는 쿠버네티스 환경을 대상으로 동적 탐지 도구와 정적 점검 도구를 결합한 통합 보안 진단 체계를 제안하며, 상용 LLM 모델을 활용한 자동 보고서 생성을 통해 인프라의 보안 운영 효율성과 실효성을 높이는 데 목표를 둔다.

Ⅰ. 서 론

SaaS(Software as a Service) 형태의 서비스가 빠르게 확산하며, 이를 제공하는 기업들은 효율적인 인프라 운영과 배포를 위해 컨테이너 기반 클라우드 인프라를 적극 도입하고 있다[1]. 이러한 흐름에 대응하기 위해 KISA(한국인터넷진흥원)는 2016년부터 CSAP(클라우드 서비스 보안인증) 인증서를 통해 서비스 제공자의 보안 및 신뢰성을 공식적으로 검증하고 있다[2].

그러나 컨테이너 기반 클라우드 인프라와 이를 조율하는 오케스트레이션 플랫폼 쿠버네티스(Kubernetes)는 높은 시스템 이해도와 복잡한 보안 구성을 요구한다. 이에 따라 보안 전담 인력과 기술 역량이 부족한 중소기업은 SaaS 환경의 안정적 운영과 보안 위협에 효과적으로 대응하기에 어렵다[3].

Ⅱ. 이론적 배경

클라우드 환경의 운영이 시작되면 중단 없이 구성을 변경하거나 점검하기 어려우므로 초기 설계 및 배포 단계에서 보안 결함을 차단하는 정적 분석은 필수적이다. 그러나 자동화, 확장성, 컨테이너 중심 동적 자원 할당 등의 특성으로 인해 다양한 형태의 예외적 위협이 발생할 수 있다.

이 진단 시스템은 초기 구성 단계의 정적 분석과 실시간 보안 이벤트 감지의 동적 탐지가 병행된 자동화 대응 체계를 통해 예상치 못한 위협에 대비하고, 시스템 구성 요소 간 안정적인 통신과 보안성을 확보하여 클라우드 보안 전략에 도움이 되고자 한다.

Ⅲ. 기술적 배경

3.1. 시스템 구성 및 기술적 배경

본 연구는 CSAP 하위 SaaS 표준 항목을 기준으로 Kubernetes 클러스터 내 보안 취약점을 진단하는 정적·동적 분석 점검 체계를 설계하였고, 그 중 일부를 [표 1]에 첨부하였다. 점검 도구는 클러스터 내 노드 및 컨테이너의 진단을 수행하고, Main Server는 수집된 결과를 분석·시각화하여 외부 LLM을 통한 보고서를 생성한다.

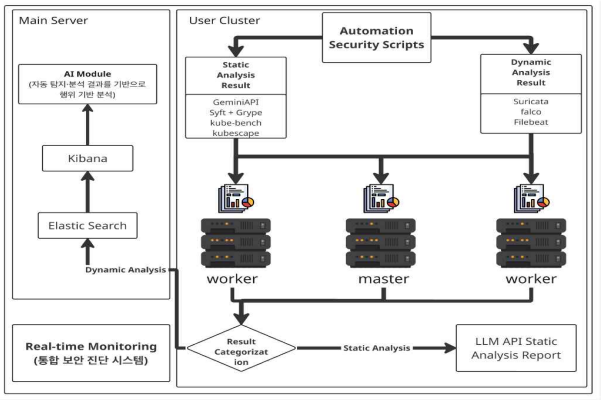
인증 기준	클라우드컴퓨팅서비스와 관련된 내·외부 네트워크에 대해 보안정책과 절차를 수립해야 한다.	
점검 목록	공통	1) 내·외부 네트워크를 통한 클라우드 시스템의 접근을 통제하는 보안 정책이 수립되어 있나?

[표 1] CSAP 보호대책 요구사항 목록 中

3.2. 통합 보안 시스템 구성도

사용자의 Kubernetes 클러스터에는 보안 진단을 수행하는 점검 도구가 배포되고, 수집된 다양한 형태의 데이터를 저장하고 분석하는 전용 Main Server가 이를 수신하고 처리한다.

전체 시스템의 동작 구조는 [Fig. 1]을 통해 나타내었으며, 해당 시스템은 VPC 환경에서 테스트 인프라 기반을 통해 기능 검증을 하였다.



[Fig. 1] 전체 시스템 구성도

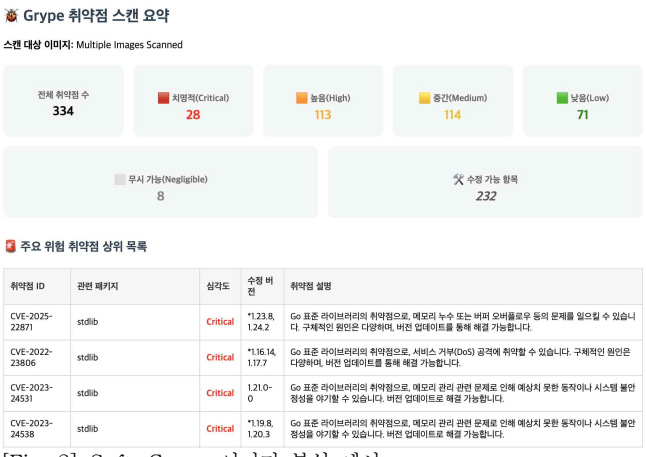
3.3. 메인 서버의 구성 및 역할

Main Server는 동적 탐지 로그의 수집과 실시간 시각화 기능을 하는 Kibana와 Elasticsearch로 구성되어 있다. 클러스터 내의 시스템 이벤트는 동적 탐지 도구를 통해 이루어지고, 실시간 검색 및 시각화의 역할을 수행한다. Main Server는 사용자 서버에 저장된 정적 보안 점검 결과 또한 수신하여 Python 스크립트와 외부의 상용 LLM API를 통해 CSAP 기준에 맞게 분석하고 요약된 보고서를 생성하는 기능을 수행한다.

3.4. 정적 점검 도구의 보안 구성 점검

정적 점검 도구는 Kubernetes 클러스터의 모든 노드와 컨테이너를 대상으로 보안 적합성을 평가하고, 네임스페이스 지정과 기능별 선택·전체 설치가 가능하다. Syft와 Grype는 이미지 내 패키지를 분석하여 CVE 기반 취약점을 진단하고, Kubescape는 IaC, RBAC, 네트워크 정책을 바탕으로 클러스터 보안 위협을 점검한다. Kube-bench는 주요 컴포넌트의 CIS 벤치마크 기준에 따라 전체 시스템의 설정 및 구성의 보안성을 평가한다.

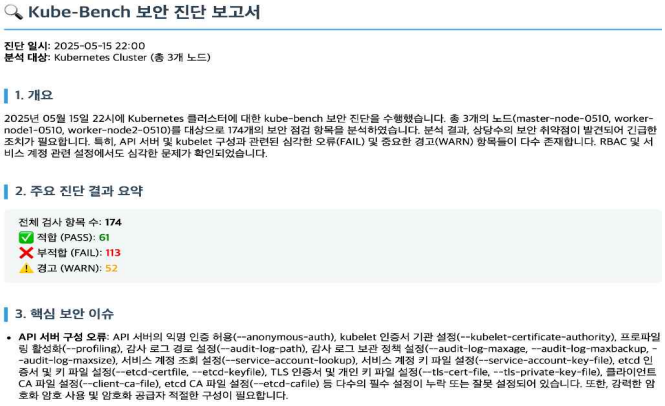
아래 [Fig. 2]는 정적 점검 도구 중 Syft와 Grype 이미지 분석 예시이다.



[Fig. 2] Syft, Grype 이미지 분석 예시

3.5. LLM을 활용한 보고서 작성

LLM의 도입을 통해 Syft, Grype, kubescape, kube-bench에서 수집된 JSON 형식의 점검 결과를 CSAP 기준에 따라 자동 분석한다. 분석된 데이터는 정제된 템플릿을 기반으로 취약점과 조치 항목이 요약된 보고서로 생성되어, 복잡한 로그와 진단 결과를 사람이 해석할 수 있는 형태로 전환하여 직관적인 가시성을 제공한다. 아래 [Fig. 3]는 상용 LLM 모델을 활용한 점검 결과 보고서의 예시를 나타낸다.

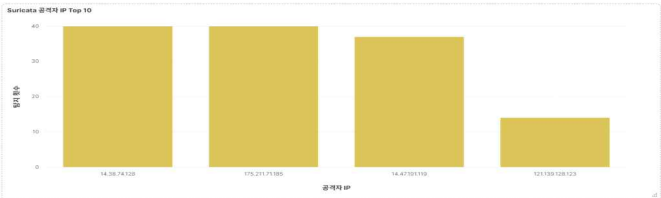


[Fig. 3] 점검 결과 보고서 中

3.6. 동적 탐지 도구의 실시간 데이터 수집·분석

동적 탐지는 Kubernetes 클러스터 내 런타임 이벤트를 실시간으로 수집·분석하여 보안 위협에 대응한다. Falco는 커널 수준의 시스템 호출을 모니터링해 컨테이너 내부의 이상 행위를 탐지하고, Suricata는 네트워크 패킷을 분석하여 잠재적 공격을 식별한다. 수집된 이벤트는 Filebeat를 통해 Main Server로 전송되며, 해당 파이프라인은 클라우드 환경의 예측 불가능한 위협을 조기에 탐지하고 분류하는 대응 체계 기능을 수행한다.

아래 [Fig. 4]는 Suricata를 통해 탐지된 공격자 IP의 예시를 보여준다.



[Fig. 4] Suricata 공격자 IP 탐지 예시

IV. 결론 및 향후 연구 방향

본 연구는 SaaS 서비스를 제공하는 중소기업체들이 기술적 난이도가 높은 Kubernetes 기반 클라우드 인프라에서 발생 가능한 위협을 체계적으로 식별하고 대응할 수 있도록 자동화된 진단 아키텍처를 설계하였다.

점검 결과는 중앙 서버에서 통합 관리되고, 시각화 및 요약 기능을 통해 복잡한 보안 데이터를 직관적으로 전달하여 인력과 자원이 제한된 중소규모 조직 및 보안 비전문가도 위협 대응력과 운영의 효율성을 확보할 수 있도록 도움이 되고자 한다.

향후 연구를 통해 머신러닝 기능을 추가하여 제공하는 보고서의 전반적인 품질을 향상하고, 정보의 정확도 고도화 및 다양한 산업 환경과 규제 조건을 반영한 보안 진단 기능을 추가하여 경량화된 배포 구조를 통해 시스템의 실용성과 범용성을 더욱 강화할 예정이다.

참 고 문 헌

[1] 퓨어스토리지(Pure Storage)와 디멘셔널 리서치(Dimensional Research), 2024. “2024년 쿠버네티스 전문가의 견해 보고서: 기업의 미래를 주도하는 데이터 트랜드”, 퓨어스토리지.

[2] 한국인터넷진흥원, 2024. ” 클라우드 보안인증제 “, Available at: https://isms.kisa.or.kr/main/csap/intro/#none

[3] 한국인터넷진흥원, 2024, “2024년 정보보호 실태조사”, 한국인터넷진흥원