8 Kubernetes 보안 강화 방법

04 Falco 소개 및 설치

소개 및 실습 내용

순서

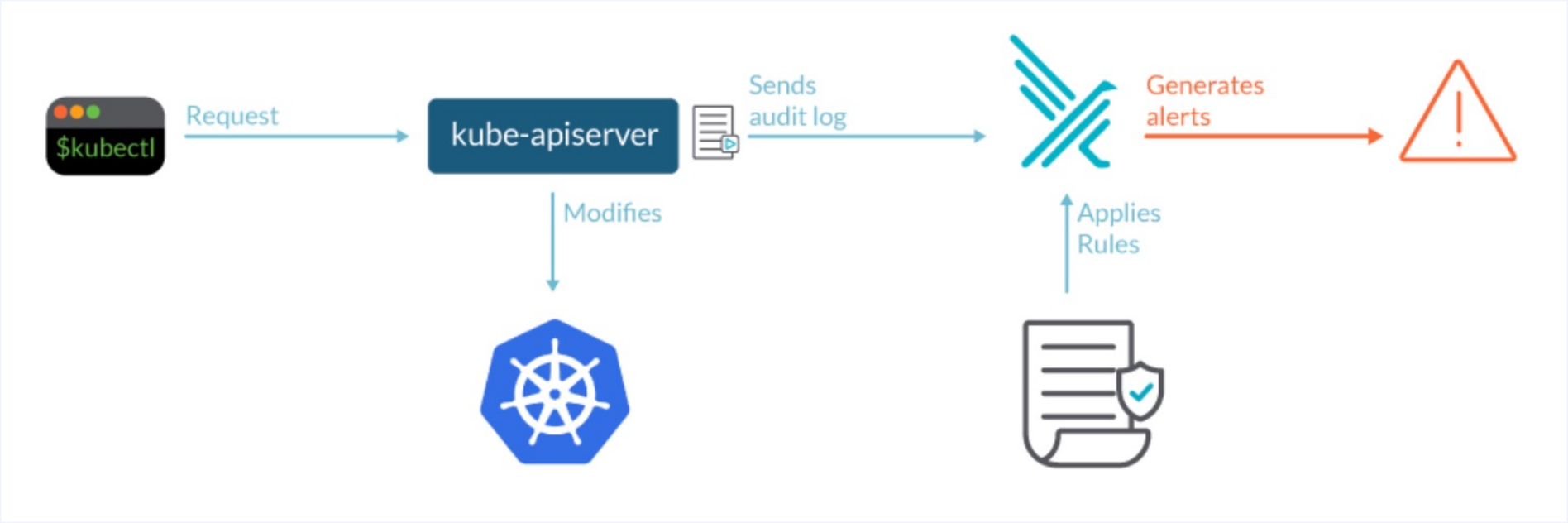
1. Falco 소개
2. 사전 준비 (EKS)
3. IAM Policy 및 Role 적용 (CloudWatch 로그 연동용)
4. Falco 설치 (Helm Chart)

실습 예제코드 경로

Chapter08 > Ch08_04-falco

1. Falco 소개 #1

Falco는 Kubernetes, 컨테이너 및 클라우드 **런타임** 전반에서 지속적인 **위험 및 위협 탐지**를 위한 **런타임 보안 관리**용 오픈소스 도구로, 지속적인 보안 감시로 예기치 않은 동작, 구성 변경, 침입 및 데이터 도난을 실시간으로 **감지 및 처리** 할 수 있음



출처 : https://sysdig.com/blog/kubernetes-audit-log-falco/

1. Falco 소개 #2

특징	상세내용
규정 준수 범위	• NIST, SOC2 또는 PCI와 같은 규정 준수 표준에 매핑되는 기본 확인 및 런타임 정책을 사용하여 규정 준수를 검증 • 커뮤니티에서 제공하는 악성 활동 및 CVE 익스플로잇 탐지를 사용하여 정책 위반을 탐지
런타임 보안 정책	• Linux 시스템 호출, Kubernetes 감사 및 클라우드 활동 로그를 통한 위협 탐지 정책 적용 • 맞춤형 정책 기반 Cloud/K8s 컨텍스트 적용 및 경고 출력 가능
자동화된 수정	• 자동화된 수정 작업(컨테이너 중지, 종료, 일시 중지)으로 Falco의 탐지 기능을 확장하여 위협에 신속하게 대응 가능 • 오픈소스 기반 에이전트를 통한 지속적인 탐지 수행 가능

2. 사전 준비 (EKS)

EKS Cluster

- 런타임 보안 검증을 위한 Kubernetes 환경
- 기존에 사용한 환경과 동일하게 사용

3. IAM Policy 및 Role 적용 (CloudWatch 로그 연동용) #1

(1) Falco 로그 대상 CloudWatch 연동용 IAM Policy 적용 명령어

- Chapter08 > Ch08_04-falco > aws

```
$ aws iam create-policy --policy-name EKS-CloudWatchLogs --
policy-document file://iam_role_policy.json
```

3. IAM Policy 및 Role 적용 (CloudWatch 로그 연동용) #2

(2) Falco 로그 대상 CloudWatch 연동용 IAM Role 적용 명령어

```
$ aws iam attach-role-policy --role-name <EKS Worker Node Role명>
--policy-arn `aws iam list-policies | jq -r '.[][] | select(.PolicyName ==
"EKS-CloudWatchLogs") | .Arn'`
```

4. Falco 설치 (Helm Chart)

(1) values.yaml 변경 내역

- Chapter08 > Ch08_04-falco > helm-chart > values.yaml
- jsonOutput: false -> true

(2) Falco Helm Chart 설치 명령어

- Chapter08 > Ch08_04-falco > helm-chart

```
$ helm install falco ./
```