8 Kubernetes 보안 강화 방법

05 Falco를 활용한 런타임 보안 강화

실습 내용

순서

1. CloudWatch 로그 수집을 위한 FluentBit 설치
2. 예제용 Deployment 배포 (Nginx)
3. 보안 취약 상황 테스트 및 CloudWatch 로그 확인
4. CloudWatch Insights를 통한 쿼리 분석

실습 예제코드 경로

Chapter08 > Ch08_05-falco-test

1. CloudWatch 로그 수집을 위한 FluentBit 설치

Fluent Bit은 매우 빠르고 가벼우며 확장성이 뛰어난 로깅 및 메트릭 프로세서 및 수집/전달 도구이다. 클라우드 및 컨테이너화된 환경 로깅용으로 널리 사용된다.

(1) FluentBit 설치 명령어

- Chapter08 > Ch08_05-falco-test > fluentbit

```
$ kubectl apply -f ./
```

2. 예제용 Deployment 배포 (Nginx)

(1) 예제용 Deployment 배포 명령어

- Chapter08 > Ch08_05-falco-test > example

```
$ kubectl apply -f deployment.yaml
```

(2) 배포후 POD 확인 명령어

```
$ kubectl get pods
```

3. 보안 취약 상황 테스트 및 CloudWatch 로그 확인 #1

(1) 특정 POD의 Bash Shell로 접속

$ kubectl exec –it <특정 POD명> -- bash

(2) 보안 정책 위배(취약점) 명령어 수행

- falco_rules.yaml > “write below etc”

$ touch /etc/2

- falco_rules.yaml > “Read sensitive file untrusted”

$ cat /etc/shadow > /dev/null 2>&1

3. 보안 취약 상황 테스트 및 CloudWatch 로그 확인 #2

(3) CloudWatch 로그 확인 경로

- CloudWatch > 로그 > 로그 그룹 > falco

(4) 로그 검색 필터링 문자열

- “Error File below /etc”
- “Warning Sensitive file opened”

3. 보안 취약 상황 테스트 및 CloudWatch 로그 확인 #3

(5) 특정 POD의 Bash Shell로 접속 (또다른 POD로 접속)

$ kubectl exec –it <특정 POD명> -- bash

(6) 보안 정책 위배(취약점) 명령어 수행

- falco_rules.yaml > “Mkdir binary dirs”

$ cd /bin

$ mkdir hello

3. 보안 취약 상황 테스트 및 CloudWatch 로그 확인 #4

(7) CloudWatch 로그 확인 경로

- CloudWatch > 로그 > 로그 그룹 > falco

(8) 로그 검색 필터링 문자열

- “Error Directory below known binary directory”

4. CloudWatch Insights를 통한 쿼리 분석 #1

(1) CloudWatch Insights 쿼리 수행 및 Dashboard 출력을 통한 분석 경로

- CloudWatch > 로그 > Logs Insights

(2) 로그 그룹 선택

- falco

4. CloudWatch Insights를 통한 쿼리 분석 #2

(3) “Mkdir binary dirs” 로그 분석을 위한 쿼리 작성

```
fields @timestamp, @message
| filter @message like 'Mkdir binary dirs'
| sort @timestamp desc
```

(4) 쿼리 실행

- 쿼리 실행 버튼 클릭

4. CloudWatch Insights를 통한 쿼리 분석 #2

(5) “Read sensitive file untrusted” 로그 분석을 위한 쿼리 작성

```
fields @timestamp, @message
| filter @message like 'Read sensitive file untrusted'
| sort @timestamp desc
```

(6) 쿼리 실행

- 쿼리 실행 버튼 클릭