**Falco란?**

OpenSource 실시간 보안 도구로 정의된 특정 행위에 대해 모니터링하는 도구이다. 2018년도 부터 시작됐고 sysdig에 의해 CNCF에 기여됬다. 보통 Falco는 시스템/서비스등을 모니터링하고 안전하게 만드는 다음과 같은 system call을 사용한다.

* Kernel로부터 실시간 Linux System Call들을 Parsing
* 강력한 정책 엔진을 사용해 stream을 확고히 함
* 정책 위반시 경보 발생

**동작원리**

커널 이벤트 모니터링하고 사전에 정의해놓은 rule에 행위상 위반되는 상황이 발생되면 경고를 발생시킨다. Falco는 Kubernetes, Linux, Cloud-Native 대상의 보안 rule set을 정의하여 사용할 수 있다.