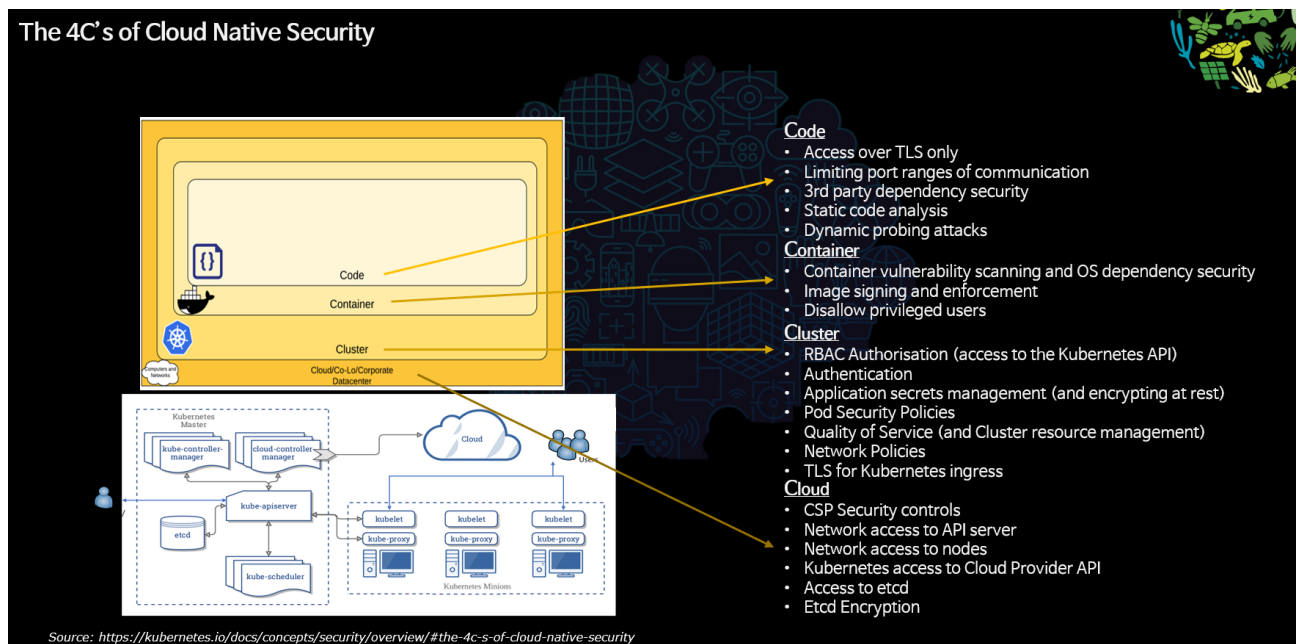


4C 개요

세상은 눈 깜짝할 사이에 계속해서 변화합니다. 어제는 클라우드 시대였고, 오늘은 클라우드 네이티브 시대로 진 입했습니다. 이 변화는 상당히 짧은 시간에 일어났을지라도 그 영향은 우리가 상상하는 것보다 훨씬 큼니다. 이 변화를 간략히 설명하자면, 인터넷이나 클라우드 환경에서 온디맨드 IT 자원을 가지고 있던 것에서 클라우드 원 칩에 기반한 소프트웨어 아키텍처를 가지고 새로운 세대의 애플리케이션을 개발하는 것으로 전환하는 것입니다.

그리고 모든 새로운 기술은 옛 기술을 무용지물로 만들려는 경향이 있듯이, 클라우드 환경에서 고도로 확장 가능 한 애플리케이션을 빌드하고 실행하기 위한 이 새로운 접근 방식도 기존의 클라우드 보안이나 네트워크 보안을 무용지물로 만들어버렸으며 부적합하게 만들었습니다. 실제로 클라우드 네이티브의 인프라에 중립적이고 개발 자 중심의 멀티 클라우드 접근 방식은 상호 연결된 도구와 플랫폼을 사용하므로 사이버 위협의 인기 대상이 되었 습니다.

그래서 점점 더 많은 기업들이 컨테이너화된 애플리케이션과 Kubernetes 투자의 가치를 극대화하기 위해 클라 우드 네이티브 방법을 채택함에 따라, 이러한 애플리케이션을 진화하는 보안 위험으로부터 보호해야 하는 필요가 중요한 역할을 하고 있습니다. 그러나 클라우드 네이티브 애플리케이션을 보호한다는 것은 그 중요한 측면을 모 두 보호하는 것을 의미하며, 이것은 말로 하는 것보다는 훨씬 어려운 과제입니다. 이 블로그에서는 각 보안 측면 과 각 측면의 모범 사례에 대해 간략하게 살펴보겠습니다.



🔄Revision #2

★Created 2 September 2023 12:04:57 by Admin

✎Updated 2 September 2023 12:16:09 by Admin