Kubernetes Security Guide

In this Kubernetes security guide we want to compile the most significant aspects of implementing Kubernetes security best practices.

Kubernetes security, like monitoring or CI/CD is becoming a must as a consequence of this platform quickly gaining reputation as the *defacto* standard for modern containerized deployments.

Unfortunately, traditional security processes need to be updated for Kubernetes; legacy security tools that were not built for containers cannot look inside, analyze or protect containers, microservices and cloud-native apps. Containers are like black boxes, useful for moving applications from development into production. They provide a great level of portability and isolation. But makes harder to understand what's happening inside, monitor and secure them. Microservices help to develop applications faster and orchestration tools like Kubernetes allow to deploy and dynamically scale the apps, but now we have different pieces moving around, therefore we must take a more dynamic security approach.

Furthermore, many organizations are adopting security best practices and implementing DevSecOps processes, where everyone is responsible for security and, security is implemented from early development stages into production through the entire software supply chain, this also known as Continuous Security.

So, moving Kubernetes to production implies new infrastructure layers, new components, new procedures and therefore new security processes and tools. This security guide will help you to implement Kubernetes security, mostly focused around Kubernetes specific security features and its configuration, but also some additionals tools that will go beyond what Kubernetes can do.

We have covered the following topics:

- Chapter 1: Understanding Kubernetes RBAC and TLS certificates
- Chapter 2: Implementing security at the pod level: Kubernetes Security Context and Kubernetes Network Policy
- Chapter 3: Securing Kubernetes components (kubelet, etcd or your registry)
- Chapter 4: Run-time security behavior monitoring: Kubernetes security policies and audit with Sysdig Falco open-source
- Chapter 5: Getting started with Falco rules for Kubernetes run-time security profiles
- Chapter 6: Implementing Kubernetes security policies and audit with Sysdig Secure over Docker's example-voting-app, a modern microservices based demo app
- Chapter 7: Hardening kube-system components with security policies

We are still working on a few new chapters, to cover static container image scanning, secret management and Kubernetes audit and compliance, stay tuned for updates!

Complete #Kubernetes security guide, RBAC, TLS, Pod Security Policies, #Docker run-time security and much more. **Click to tweet**

You can use this guide as comprehensive read if you are new to Kubernetes security or as a quick reference document / cheat sheet if you are looking at implementing specific Kubernetes security best practices.

If you are new into Docker and container security, as a prerequisite for this guide, we recommend you to check out 7 Docker security vulnerabilities and threats.

Additionally, we also wrote some real stories about Kubernetes security incidents that will help you understand the threats that you need to consider:

- Fishing for Miners - Cryptojacking Honeypots in Kubernetes.
- Detecting cryptojacking with Sysdig Falco open-source.