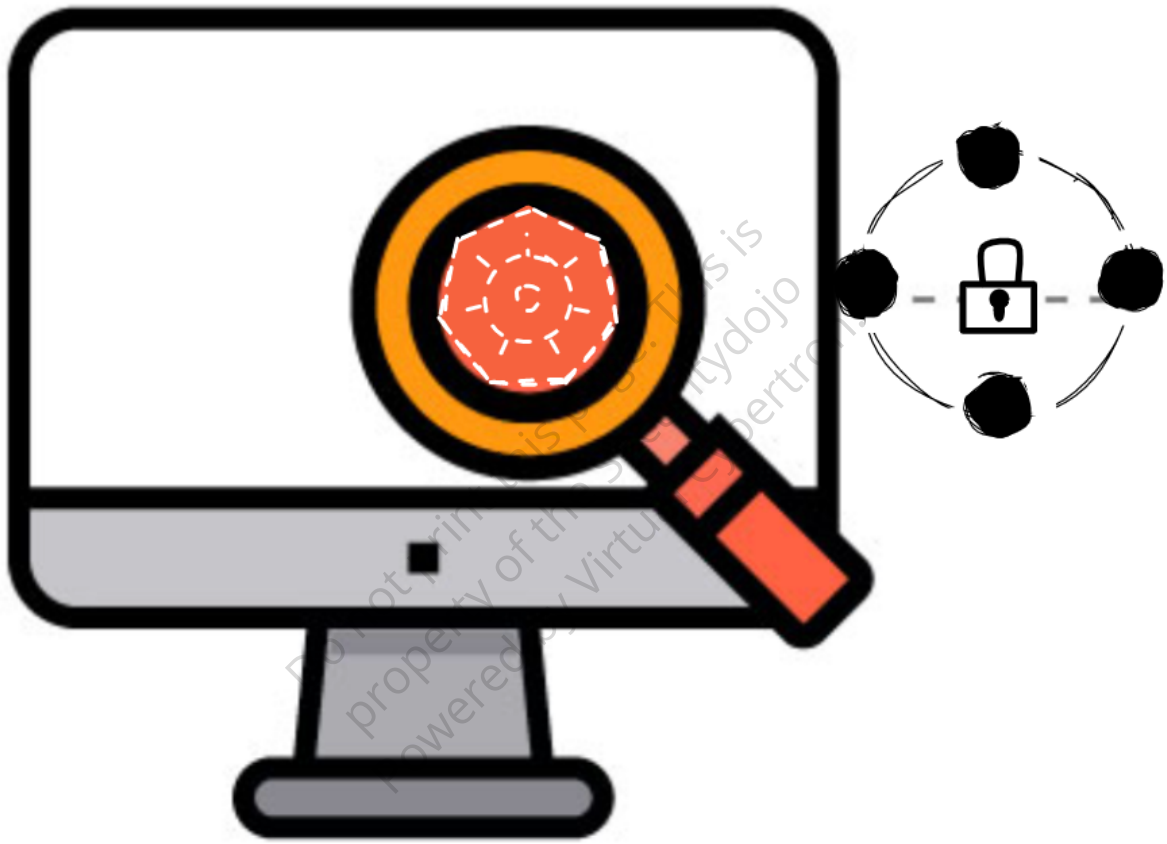
Automated Vulnerability Analysis of Kubernetes



Automated vulnerability analysis in Kubernetes refers to integrating security tools and techniques in pipelines to identify security vulnerabilities, misconfigurations, and potential risks within Kubernetes environments. It improves the security posture of kubernetes cluster. Alongside we can integrate custom remediations functions to mitigate the vulnerabilities. Organisation can follow the below practices for vulnerability analysis:

- Automated scanning the environment (CIS Benchmarks)
- Analysing the reports and identify the vulnerabilities
- Define the severity based on risk

- Take recommended Remediations
- Automate it(if possible)
- Continuous Monitoring

By incorporating above practices into the Kubernetes deployment lifecycle, organizations can proactively identify and mitigate security risks, improve their overall security posture, and minimize the risks of attacks and data breaches.

CIS Kubernetes Benchmark

A comprehensive set of guidelines called the CIS (Centre for Internet Security) Kubernetes Benchmark offers best practises for setting up a Kubernetes cluster safely.

- The benchmark encompasses more than 120 security checks that scrutinize various aspects of your Kubernetes cluster.
- For businesses wishing to improve their Kubernetes security and adhere to accepted industry best practises, the CIS Kubernetes Benchmark is a priceless tool. It offers a thorough, step-by-step tutorial for securing each component of a Kubernetes cluster, including the worker nodes, control plane, and everything in between.
- A number of cybersecurity experts and enthusiasts worked together to create the CIS Kubernetes Benchmark.
- There are also customised versions of the CIS Kubernetes Benchmark created especially for managed Kubernetes services like Amazon's Elastic Kubernetes Service (EKS) and Google's Google Kubernetes Engine (GKE).

Reference: @magnologan