Product Requirements Document

(Container Vulnerability Scanner)

Presented By
Karthika

KUBERNETES SECURITY SCAN

A technical exploration of detecting vulnerabilities and misconfigurations in Kubernetes clusters.

91-9677125179

Chennai

Karthika2406@gmail.com

www.karthika2406.com

Problem

The organization faces several operational challenges, including a lack of a centralized collaboration system, inefficient scheduling and resource utilization, the absence of real-time project tracking, and delays in reporting and deliverable completion.

Proposed Solution

Build a security scanner tool to identify risks, generate reports, and provide remediation steps.

Expected Outcome

Improved cluster security, reduced risk exposure, automated compliance checks.

Conclusion

The scanner provides a scalable and automated way to secure Kubernetes workloads, ensuring stronger resilience.

Technical (GoLang + Docker + K8s)

Build a tiny web app that shows current date & time, containerize it, deploy to Kubernetes, and expose it on the internet.

Challenges

- Package a Go app reproducibly
- Publish an image for others to run
- Run multiple replicas reliably
- Make the app reachable from WAN

Solution

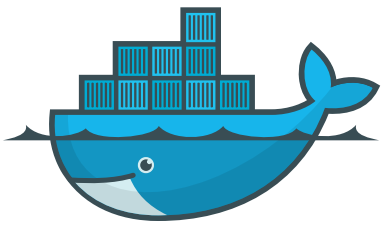
- Use a tool like Kubescape to scan
- Summarize by severity & control
- Export JSON results

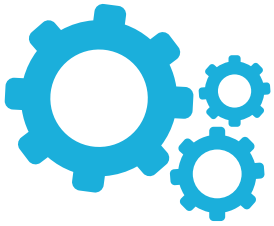
Steps

- Start cluster (Minikube/K3s)
- Install Kubescape
- kubescape scan --format json --output results.json
- Attach JSON as deliverable

Deliverables

- results.json (scan output)
- Short summary: Critical/High/Medium/Low counts





PRODUCT & TECHNICAL CASE STUDY

GOLANG, DOCKER, AND KUBERNETES IMPLEMENTATION

Presented By
Karthika