Automating container runtime security scanning with Snyk

Pas Apicella
Principal Solution Engineer APJ
pas@snyk.io
@PasApicella
Developer Security Platform

Snyk Code

Snyk Open Source

Snyk Container

Snyk IaC

Developer Experience

Application intelligence

Security intelligence

Empowerment

Extensibility

Governance
What do we mean when we say, “Kubernetes application security”?

• Vulnerabilities in container images
  • In your proprietary code
  • In your application’s dependencies
  • In the container’s OS (Linux) packages
• Infrastructure-as-code misconfigurations
  • These can drastically increase the blast radius of potential exploits!
What does Snyk’s Kubernetes monitor do?

1. Scans the container image associated with each workload for vulnerabilities
2. Prioritizes vulnerabilities based on runtime configuration
3. Monitors for new vulnerabilities by re-scanning daily and alerting

Workload types supported:

- Deployments
- ReplicaSets
- DaemonSets
- StatefulSets
- Jobs
- CronJobs
- ReplicationControllers
- Pods
On board Kubernetes workloads to Snyk

1. Manually via Snyk UI (Integrations > Kubernetes)
2. API call to Import Projects
3. Add the “orgs.k8s.snyk.io/v1” annotation to a workload (Deployment, Job, ReplicaSet, Pod, etc.)
4. Add the annotation to an entire Namespace
5. Define a custom policy in Rego (Today’s Demo!!!!)
Today's Demo with Snyk and Kubernetes

- Snyk SCM Scan
- Snyk CR Scan
- Snyk Platform
- Security Specialist
- Snyk K8s Integration (Auto Import/Delete)

- GitHub
- Google Container Registry
- Snyk Controller
- Pod
- ReplicaSet
- Deployment
- Snyk IaC Scan
- Rego Policy Language

- GKE
- Platform Operator
- Open Policy Agent
Today's Demo with Snyk and Kubernetes

Snyk Platform

Snyk SCM Integration

Snyk IDE Integration
Live Demo Time
Visit us at our Snyk Booth