RedHat Advanced Cluster Security and herding Goats

Introduction

Mark Freer
mfreer@redhat.com

Red Hat

Agenda

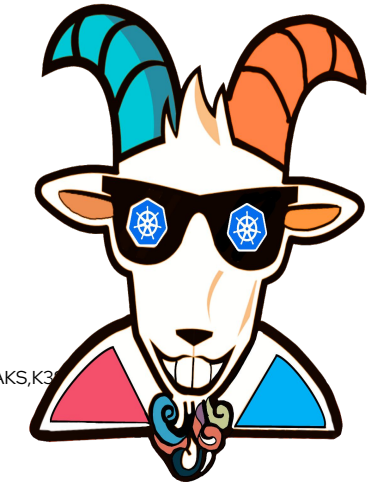
Introduction

- - Overview of Kubernetes security challenges.
- - Introduction to Red Hat Advanced Cluster Security (ACS) and Kubernetes Goat.
- **Objective**
- - Demonstrate the effectiveness of ACS in identifying and suggesting fixes for vulnerabilities within a Kubernetes cluster.
- - Show how these practices can be integrated into an SRE team's incident management process.
- **Demo time**
- - Brief on Kubernetes Goat and its purpose as a vulnerable cluster for educational purposes.
- - Steps to set up Kubernetes Goat in a safe, isolated environment.
- **Integrating Red Hat ACS**
- - Overview of ACS and its capabilities.
- - Steps to integrate ACS with Kubernetes Goat.
- - Configuring ACS to scan for vulnerabilities.

Agenda

- **5. Demonstration**
- - Live or recorded demo of ACS scanning Kubernetes Goat.
- - Highlighting key vulnerabilities discovered by ACS.
- **Incorporating Findings into Incident Management**
- - How to interpret ACS reports.
- - Integrating ACS findings into an existing incident management process.
- - Tooling and automation for efficient vulnerability

What is Kubernetes Goat



- The Kubernetes Goat project is designed to be an intentionally vulnerable cluster environment.
- It support to run on all kinds (no-pun intended) of of Kubernetes Environment like Openshift, GKE, EKS,AKS,K3
- Specifically to exploit but not limit to the following vulnerability scenarios.
  - Sensitive keys in codebases
  - DIND (docker-in-docker) exploitation
  - SSRF in the Kubernetes (K8S) world
  - Container escape to the host system
  - Docker CIS benchmarks analysis
  - Kubernetes CIS benchmarks analysis
  - Attacking private registry
  - NodePort exposed services
  - Helm v2 tiller to PwN the cluster - [Deprecated]
  - Analyzing crypto miner container
  - Kubernetes namespaces bypass
  - Gaining environment information
  - DoS the Memory/CPU resources
  - Hacker container preview
  - Hidden in layers
  - RBAC least privileges misconfiguration
  - Kube Audit - Audit Kubernetes clusters
  - Falco - Runtime security monitoring & detection
  - Popeye - A Kubernetes cluster sanitizer
  - Secure network boundaries using NSP
  - Cilium Tetragon - eBPF-based Security Observability and Runtime Enforcement
  - Securing Kubernetes Clusters using Kyverno Policy Engine

How SRE use ACS

In this presentation, I will discuss our Red Hat Advanced Cluster Security tooling and how our SRE teams incorporated it into our Incident Management process and tooling accelerated our response to Critical Vulnerability Exploits (CVE's).

Slide title should not exceed one line

Optional subheading

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean eleifend laoreet eros, eu molestie arcu tempus ac.

- Etiam interdum nunc non venenatis rutrum
- Phasellus venenatis sem ac vulputate facilisis
- Quisque vitae nisl accumsan aliquet

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean eleifend laoreet eros, eu molestie arcu tempus ac.

- Etiam interdum nunc non venenatis rutrum
- Phasellus venenatis sem ac vulputate facilisis
- Quisque vitae nisl accumsan aliquet

Source:
Insert source data here
Insert source data here
Insert source data here

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.


linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat

Red Hat