Cloud Platform Automation Internship

By: Alisa Lu & Liberty Vanty

About Us

Liberty Vanty

University of Virginia
Computer & Data Science
Fourth Year

Alisa Lu

Texas A&M
Computer Science
Junior

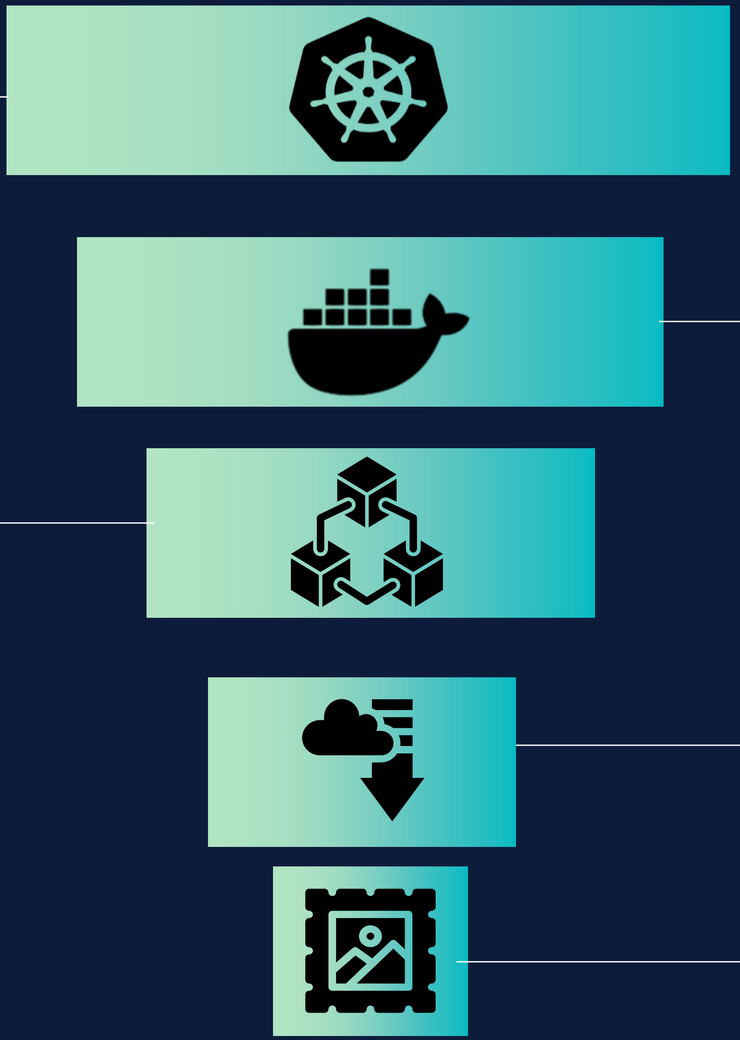
Cloud Platform Automation

Our team is in the process of deploying Kubernetes clusters to each and every store! These clusters host the applications the team needs.

Technology

Kubernetes, Kyverno
Trivy, Docker
Azure, GitHub
PowerShell, YAML

Architecture Overview



Kubernetes

Automates deployment, scaling, and management for containerized applications

Docker

A container management tool that ensures the application runs the same wherever it is deployed

Containers

Used to package applications in an isolated environment that includes everything needed to run applications

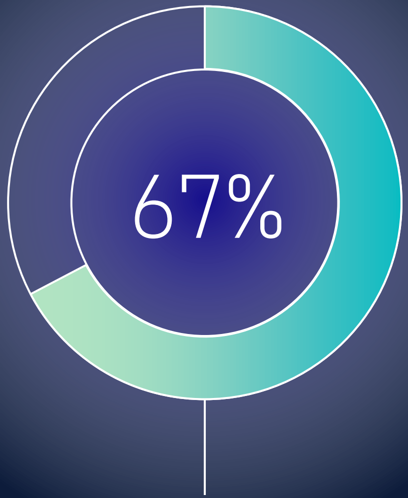
Registries

Sites where container images are stored for developers to use and distribute

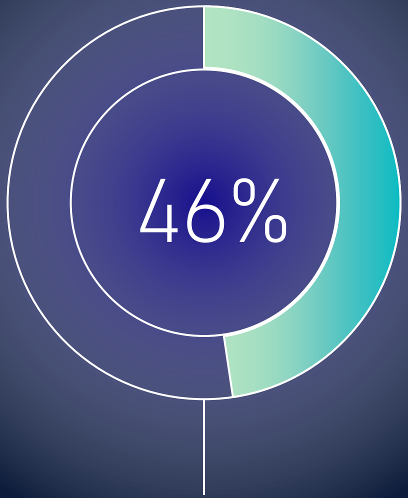
Image

Static code blueprint for creating containers

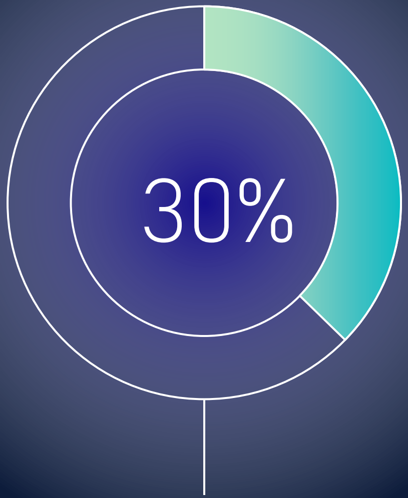
Container Security: Why it Matters



Delayed or slowed down deployment due to Kubernetes security concerns



Experienced revenue or customer loss due to a container or Kubernetes security incident



Faced fines, legal action, or lawsuits due to Kubernetes security breaches

Red Hat. *The State of Kubernetes Security Report, 2024 Edition*.

Top Concerns

Vulnerable Application Components

Insecure Container Images

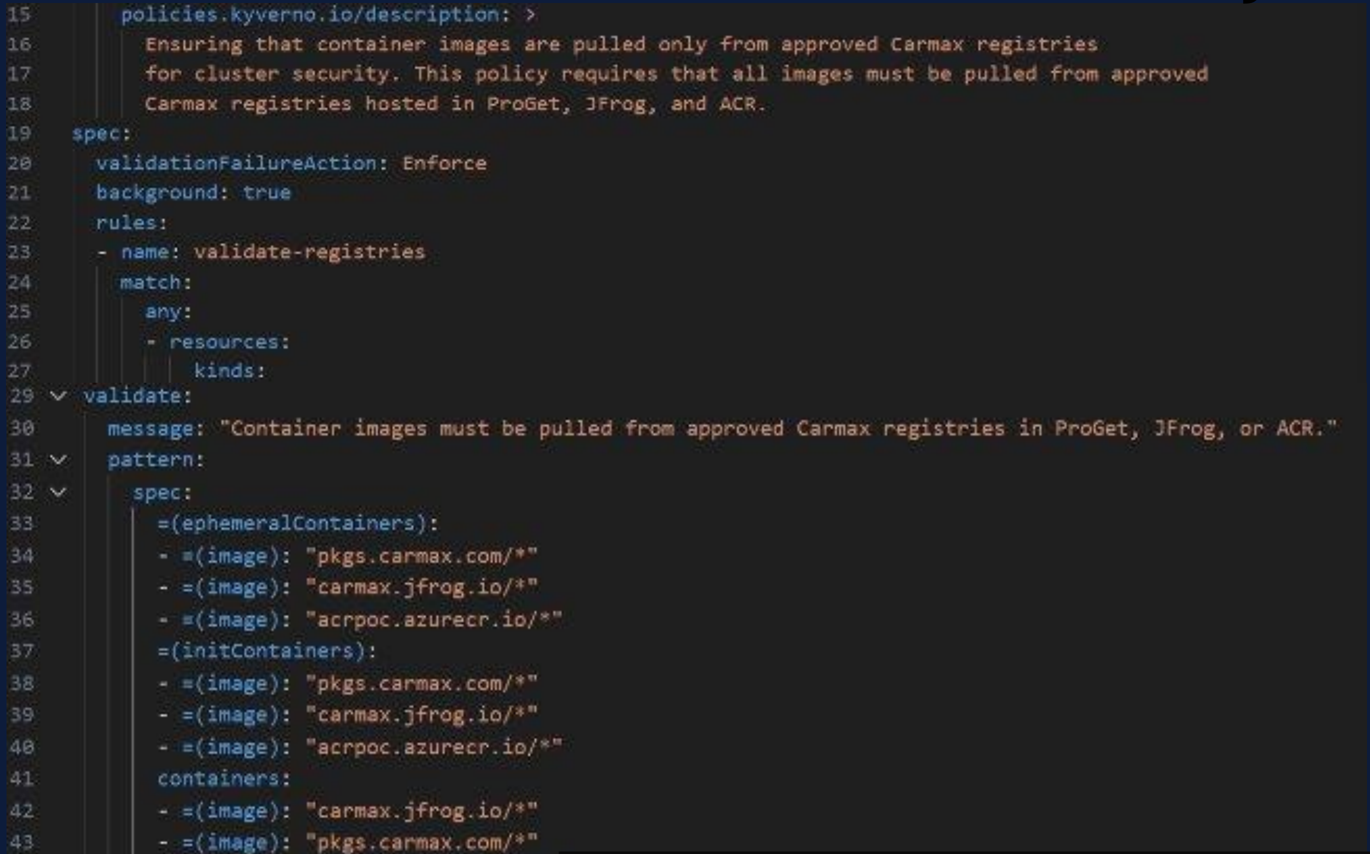
Red Hat. *The State of Kubernetes Security Report, 2024 Edition*.

Our Solution

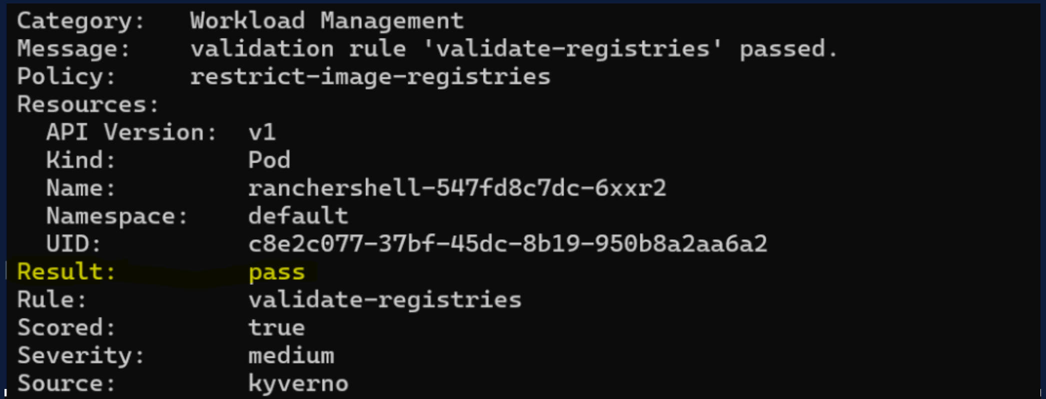
By implementing cybersecurity measures with the Kyverno policy engine, we can protect CarMax containers and deployments from vulnerable images.

Our policy restricts image pulling capabilities to authorized registries only. An example would be ProGet, ACR, and JFrog.

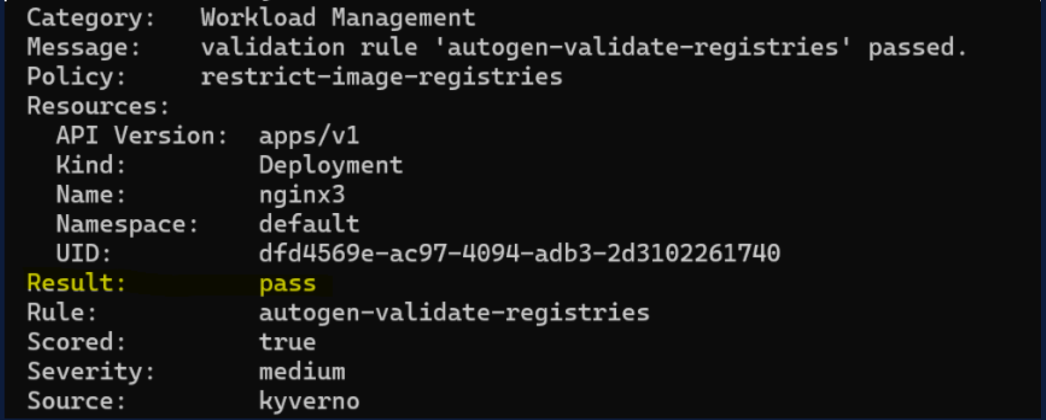
Our Policy Results



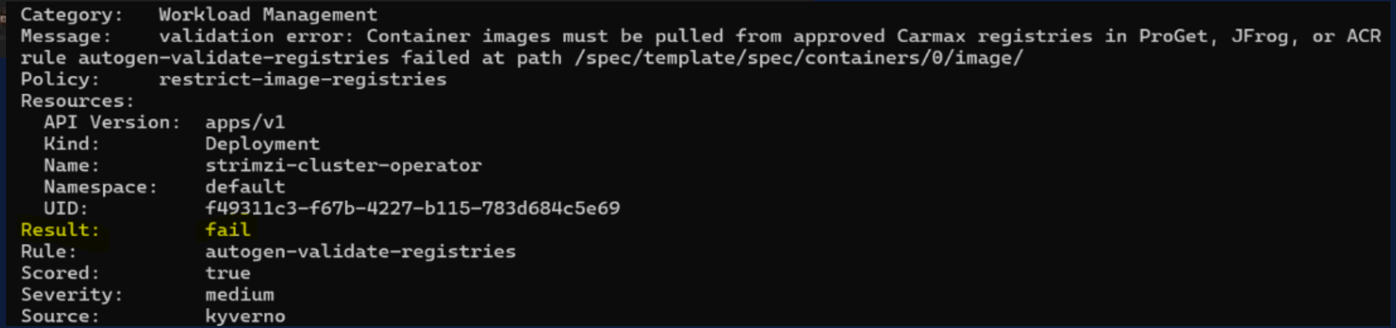
```
    policies.kyverno.io/description: >
      Ensuring that container images are pulled only from approved Carmax registries
      for cluster security. This policy requires that all images must be pulled from approved
      Carmax registries hosted in ProGet, JFrog, and ACR.
spec:
  validationFailureAction: Enforce
  background: true
  rules:
  - name: validate-registries
    match:
      any:
      - resources:
          kinds:
    validate:
      message: "Container images must be pulled from approved Carmax registries in ProGet, JFrog, or ACR."
      pattern:
        spec:
          =(ephemeralContainers):
          - =(image): "pkgs.carmax.com/*"
          - =(image): "carmax.jfrog.io/*"
          - =(image): "acrpoc.azurecr.io/*"
          =(initContainers):
          - =(image): "pkgs.carmax.com/*"
          - =(image): "carmax.jfrog.io/*"
          - =(image): "acrpoc.azurecr.io/*"
          containers:
          - =(image): "carmax.jfrog.io/*"
          - =(image): "pkgs.carmax.com/*"
          - =(image): "acrpoc.azurecr.io/*"
```



```
Category:   Workload Management
Message:    validation rule 'validate-registries' passed.
Policy:     restrict-image-registries
Resources:
  API Version:  v1
  Kind:         Pod
  Name:         ranchershell-547fd8c7dc-6xxr2
  Namespace:    default
  UID:          c8e2c077-37bf-45dc-8b19-950b8a2aa6a2
Result:         pass
Rule:           validate-registries
Scored:         true
Severity:       medium
Source:         kyverno
```



```
Category:   Workload Management
Message:    validation rule 'autogen-validate-registries' passed.
Policy:     restrict-image-registries
Resources:
  API Version:  apps/v1
  Kind:         Deployment
  Name:         nginx3
  Namespace:    default
  UID:          dfd4569e-ac97-4094-adb3-2d3102261740
Result:         pass
Rule:           autogen-validate-registries
Scored:         true
Severity:       medium
Source:         kyverno
```



```
Category:   Workload Management
Message:    validation error: Container images must be pulled from approved Carmax registries in ProGet, JFrog, or ACR
rule autogen-validate-registries failed at path /spec/template/spec/containers/0/image/
Policy:     restrict-image-registries
Resources:
  API Version:  apps/v1
  Kind:         Deployment
  Name:         strimzi-cluster-operator
  Namespace:    default
  UID:          f49311c3-f67b-4227-b115-783d684c5e69
Result:         fail
Rule:           autogen-validate-registries
Scored:         true
Severity:       medium
Source:         kyverno
```

Our Solution

By creating documentation and basic scripts on open-source software Trivy, our team is now equipped to perform regular vulnerability scans on all images within a Kubernetes cluser.

Other Work

Venafi is a certificate management tool. When used with Kubernetes, Venafi can automate the process of renewing and revoking certificates.

We wrote documentation on the integration between Venafi and Kubernetes within the company for the automation of the certificate lifecycle.