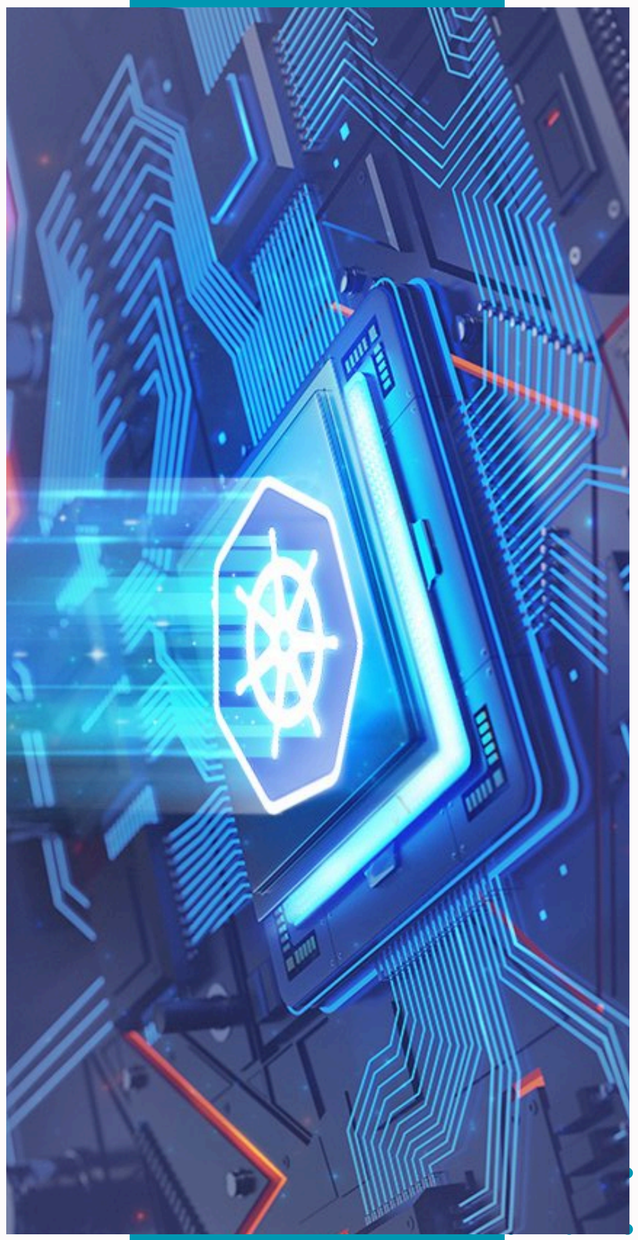
ASEAN CYBER SHIELD

BUILDING A KUBERNETES CLOUD SECURITY INFRASTRUCTURE

Present by: AnonyMeow

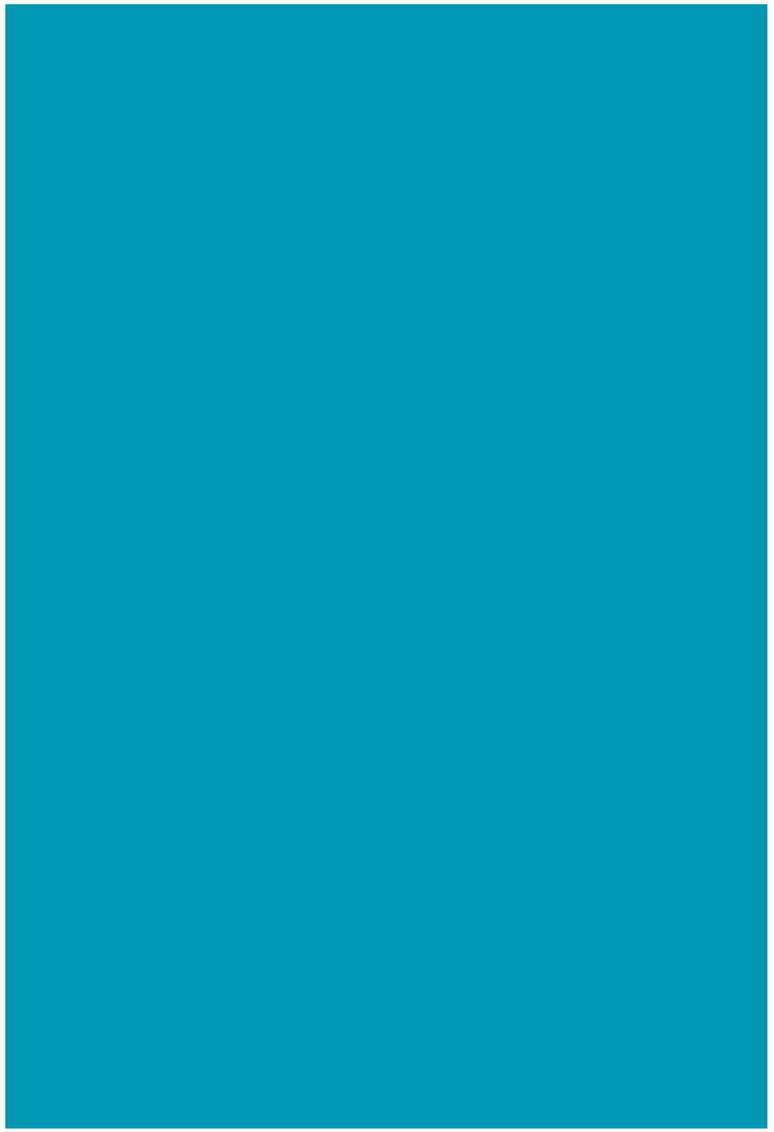


KISA Korea Internet & Security Agency

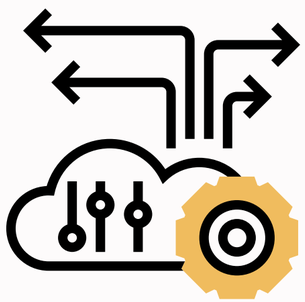
AKCF

August, 30 2024

Content



Mid-project Progress



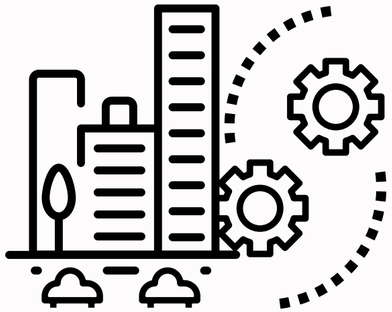
Application Deployment

Sample application has been successfully deployed to the Kubernetes cluster.

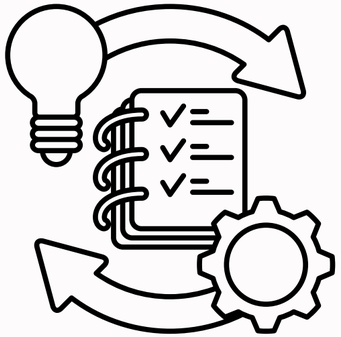
Kubernetes Infrastructure

Kubernetes infrastructure have been installed
and setup

- Helm
- Cert-Manager
- Load Balancer
- NGINX Ingress Controller



Security Implementation



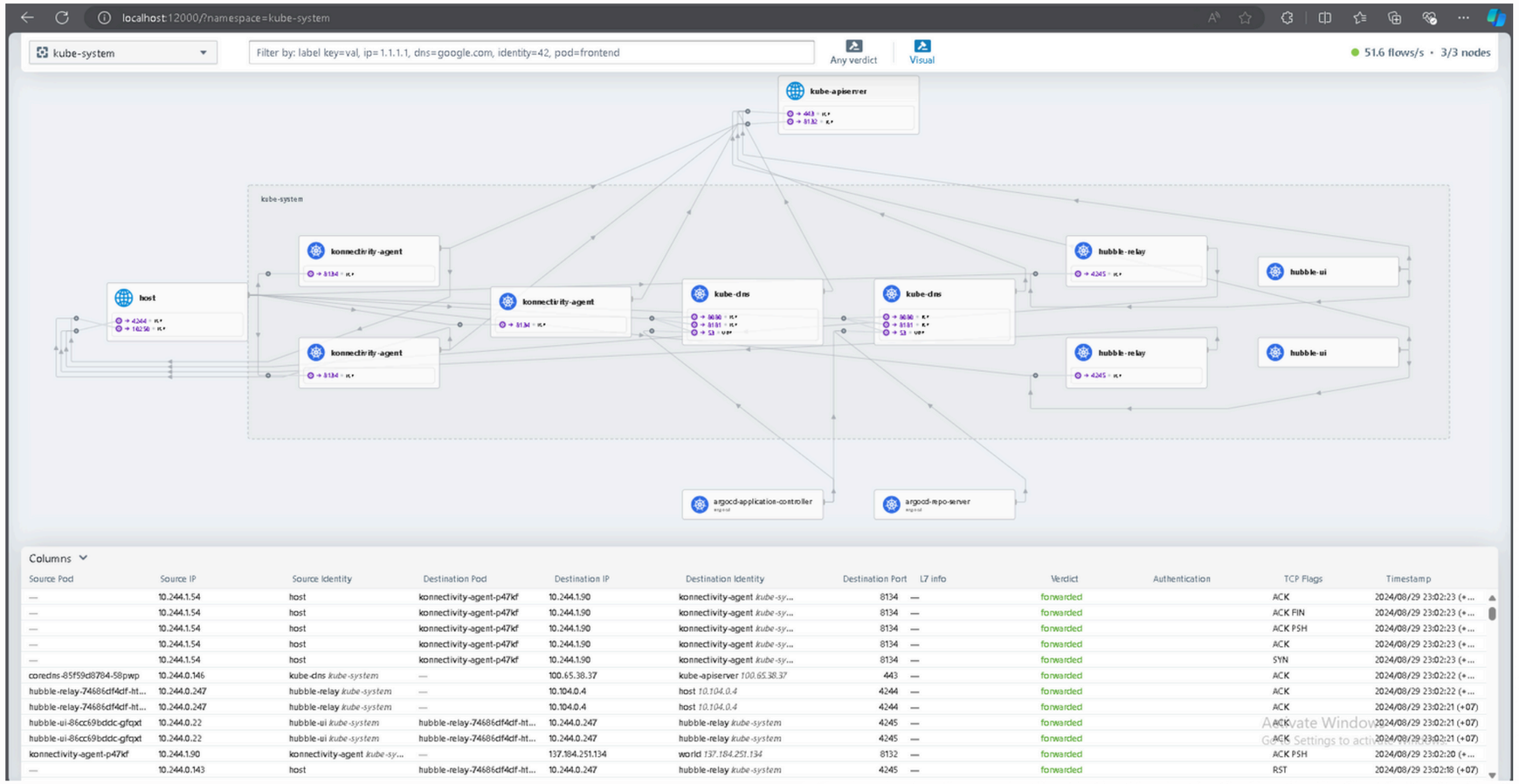
Kubernetes infrastructure have been installed and setup

- Cotainer Runtime Security
- Encryption in Transit
- NGINX Ingress Configuration
- Kubernetes Secrets

Security Implementation

Securing Network

- Used **VPC** on DigitalOcean to create an **isolated** network environment
- Implemented **Cilium** and **Hubble** to enhance network security and provide deep observability
- **Cilium** enhances the security posture of our Kubernetes cluster, ensuring that only authorized services can communicate with each other
- **Hubble** allows us to monitor and observe network traffic in real time, helping us to identify potential security issues and optimize network performance

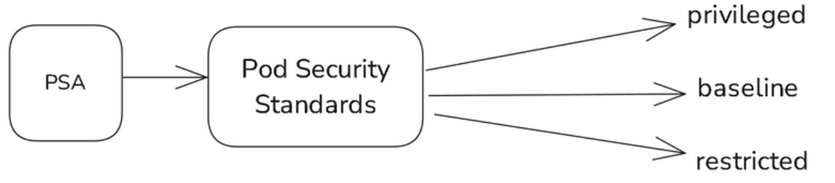


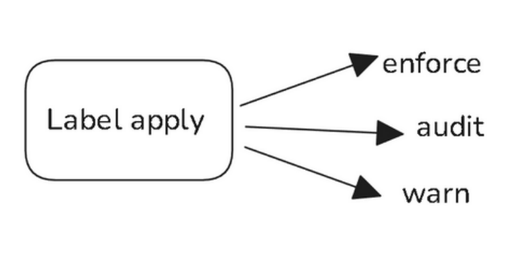
Security Implementation

Prevent Pod Privilege

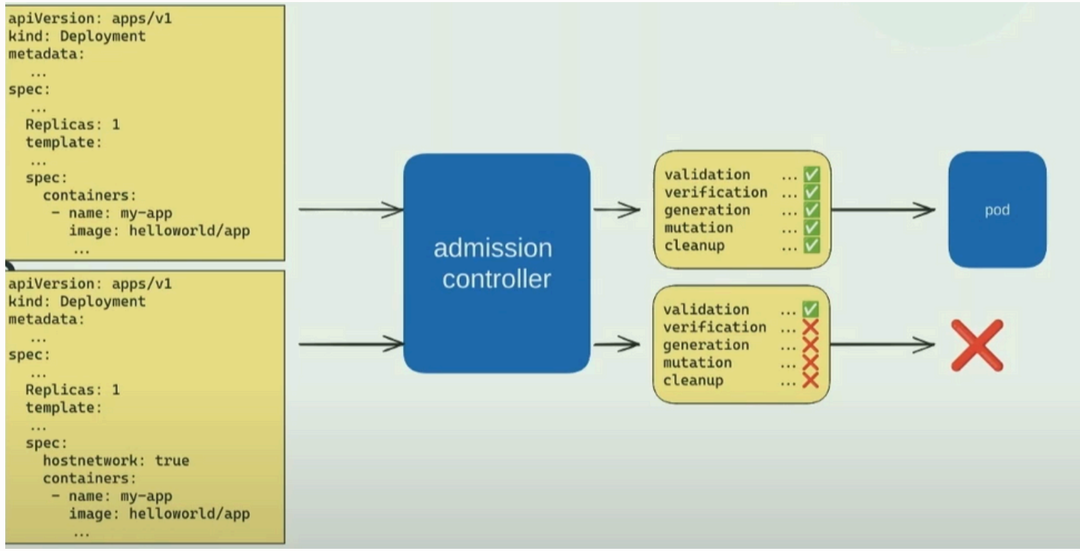
```
    securityContext:
      runAsNonRoot: true  # Ensure non-root user
      runAsUser: 1000
      runAsGroup: 3000
      fsGroup: 2000
      allowPrivilegeEscalation: false
      readOnlyRootFilesystem: true
      seccompProfile:         # Adding seccompProfile
        type: RuntimeDefault
      capabilities:
        drop:
        - ALL
```

Prevent Pod Privilege (Cont.)





Pod security admission

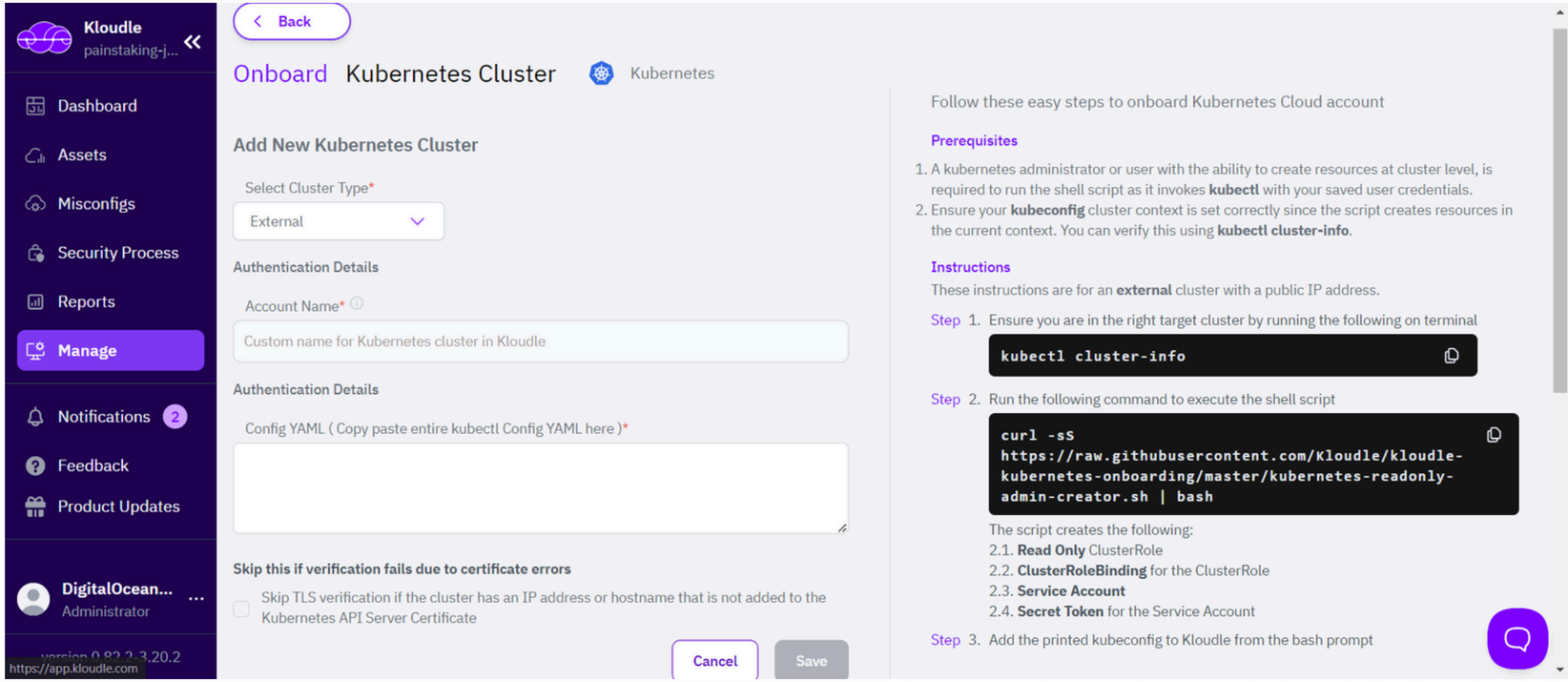



```
kubectl label --overwrite ns argocd pod-security.kubernetes.io/enforce=restricted
kubectl label --overwrite ns cert-manager pod-security.kubernetes.io/enforce=restricted
kubectl label --overwrite ns flask-app pod-security.kubernetes.io/enforce=restricted
kubectl label --overwrite ns ingress-nginx pod-security.kubernetes.io/enforce=restricted
```

Cloud Security Scanning(Kloudle)

Kloudle is a cloud security tool designed to help organizations identify and manage security risks across their cloud environments.

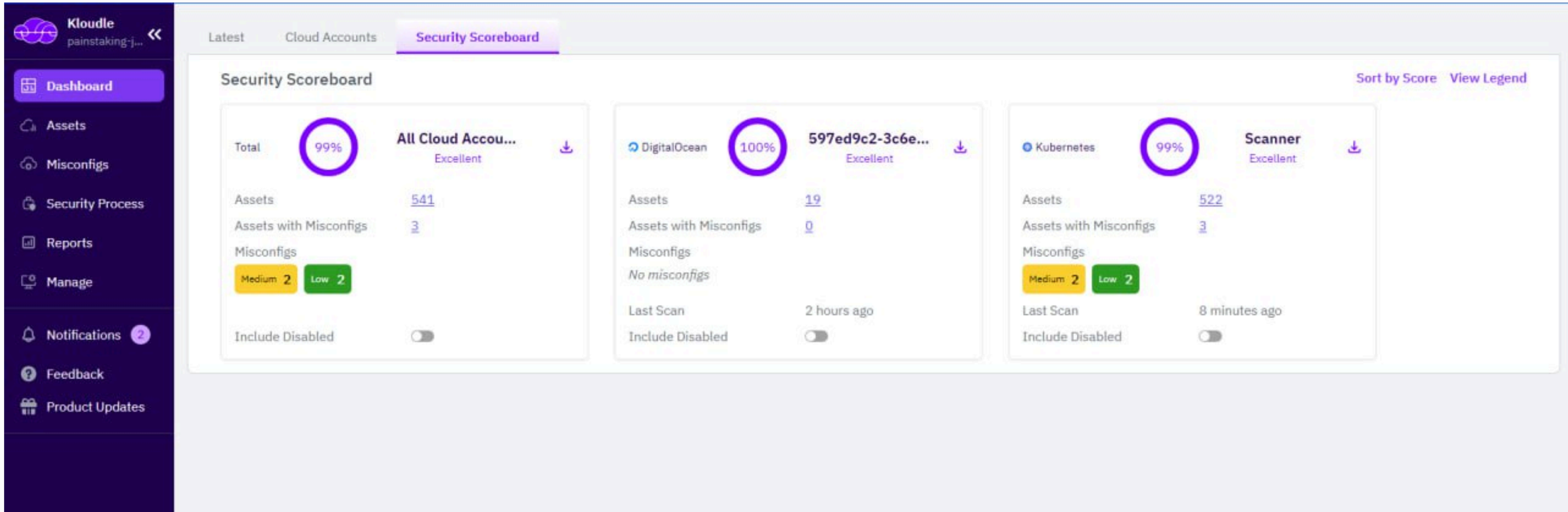
To ensure our Kubernetes infrastructure, we integrated Kloudle as part of our security testing process. Kloudle is a cloud-native security tool that helps in identifying and mitigating security risks across cloud environments (DigitalOcean), including Kubernetes.



Project Result

Security Overview for Kubernetes:

- Score: The Kubernetes cluster received a security score of 99%.
- Misconfigurations: The scan detected 3 assets:
  - Medium Severity: 2 misconfigurations.
  - Low Severity: 2 misconfigurations



What have we Learned from this project?

- Solid understanding of Kubernetes architecture and core components.
- Focused on container orchestration, resource management, and security.
- Explored RBAC, network policies, and cloud security in Kubernetes.
- Emphasized container security and policy enforcement tools.
- Learned automation through CI/CD pipelines and IaC.
- Recognized the importance of monitoring and auditing for compliance.

What skills did we experience in this project?

- Improved Kubernetes administration by deploying, managing, and scaling clusters.
- Configured security settings and networking policies.
- Implemented cloud security best practices and secured Kubernetes components.
- Enhanced Docker and container security knowledge.
- Gained hands-on experience with CI/CD and security automation.
- Strengthened knowledge of Kubernetes security.

Difficulty in Understanding the Concept and Implementation

Time-Consuming

Issue

Complex Technology Integration

Troubleshooting Errors

THANK YOU