# TOP 5 KUBERNETES SECURITY ATTACK VECTORS

**Aravind Shilam**

# INTRODUCTION

- **Kubernetes is widely used but comes with security risks.**
- **Misconfigurations can lead to severe breaches.**
- **Importance of securing Kubernetes clusters.**
- **Overview of the top 5 attack vectors.**

# ATTACK VECTOR #1 - MISCONFIGURED RBAC (ROLE-BASED ACCESS CONTROL)

- **Weak RBAC permissions allow privilege escalation.**
- **Attackers can gain unauthorized access.**
- **Best practice: Follow the principle of least privilege.**
- **Use role bindings carefully to avoid privilege misuse.**

# ATTACK VECTOR #2 - INSECURE API SERVER EXPOSURE

- **API server is the control plane entry point.**
- **Unrestricted access can lead to cluster takeover.**
- **Best practice: Implement strong authentication & authorization.**
- **Use network policies to restrict API access.**

# ATTACK VECTOR #3 - CONTAINER ESCAPES

- **Attackers exploit container vulnerabilities to access the host.**
- **Misconfigured privileged containers increase risks.**
- **Best practice: Use least privilege containers.**
- **Enforce sandboxing to isolate workloads.**

# ATTACK VECTOR #4 - IMAGE SUPPLY CHAIN ATTACKS

- **Malicious or vulnerable images pose security threats.**
- **Attackers can inject malware through unverified images.**
- **Best practice: Use trusted registries and image signing.**
- **Regularly scan images for vulnerabilities.**

# ATTACK VECTOR #5 - NETWORK POLICY MISCONFIGURTIONS

- Open communication between pods allows lateral movement.
- Unrestricted pod-to-pod communication increases risks.
- Best practice: Define strict network policies.
- Implement zero-trust network segmentation.

# THANK YOU

**Aravind Shilam**