Kubernetes Phase 2 Remediation Actions Documentation

# 1. Network Policy Remediation

Configuration File: baseline\_networkpolicy.yaml

Description:Applies a baseline NetworkPolicy to deny all ingress traffic by default.

Remediation Command:  
kubectl apply -f baseline\_networkpolicy.yaml

Purpose:Ensures pods are not accessible unless explicitly allowed, reducing lateral movement risks.

# 2. Seccomp Profile Enforcement

Configuration File:seccomp\_profile.yaml

Description:Applies a PodSecurityPolicy or equivalent SecurityContext to enforce seccomp profiles (e.g., RuntimeDefault).

Remediation Command:  
kubectl apply -f seccomp\_profile.yaml

Purpose:Limits syscalls accessible to containers, reducing kernel attack surface.

# 3. Capabilities and Privileges Remediation

Configuration File: baseline\_capabilities.yaml

Description: Defines container security context to drop dangerous Linux capabilities (ALL, or specific ones like NET\_RAW).

Remediation Command:  
kubectl apply -f baseline\_capabilities.yaml

Purpose:Hardens containers by limiting their ability to perform sensitive operations.

# 4. SELinux or AppArmor Profile Enforcement

Configuration File:baseline\_apparmor.yaml or baseline\_selinux.yaml

Description:Applies security profiles (e.g., AppArmor or SELinux) to restrict container behavior.

Remediation Command:  
kubectl apply -f baseline\_apparmor.yaml

Purpose:Limits system access per pod/container, enforcing least privilege.

# 5. Audit Logging Enforcement

Configuration File:Not directly shown

Description:Configures Kubernetes API server to enforce and forward audit logs.

Remediation Command:  
--audit-log-path=/var/log/kubernetes/audit.log  
--audit-policy-file=/etc/kubernetes/audit-policy.yaml

Purpose:Enables forensic analysis and compliance tracking.

# 6. RBAC Lockdown

Configuration File:Implied via Role/ClusterRole YAMLs

Description:Removes over-permissive ClusterRoleBindings or reduces RBAC scope.

Remediation Command:  
kubectl delete clusterrolebinding overly-permissive-binding

Purpose:Limits user/service account permissions in alignment with least privilege.

# 7. API Server Hardening

Configuration File:Configuration flags

Description:Disables anonymous access and insecure ports on the API server.

Remediation Command:  
--anonymous-auth=false  
--insecure-port=0

Purpose:Prevents unauthorized access and strengthens cluster security posture.