AEGIS VETIS · CHECKLIST

30 contrôles de sécurité Kubernetes pour la conformité NIS2 / SecNumCloud

Issu des policies baseline Aegis Vetis. Chaque contrôle est automatisable via Kyverno et scoré contre les référentiels NIS2, SecNumCloud (mentions inspirées) et CIS Kubernetes Benchmark.

Cette checklist couvre la posture minimale attendue d'un cluster Kubernetes en production. Imprimez-la, partagez-la avec vos équipes Ops et Sécurité, et utilisez-la comme grille d'auto-évaluation lors de votre prochain comité de sécurité.

1. POD SECURITY & CONTAINER HARDENING

- ☐ Aucun pod ne tourne avec `securityContext.privileged: true`
- ☐ Aucun pod ne tourne en `runAsUser: 0` (root)
- ☐ `readOnlyRootFilesystem: true` sur les workloads applicatifs
- ☐ `allowPrivilegeEscalation: false` partout
- ☐ `capabilities.drop: [ALL]` par défaut, ajout explicite uniquement
- ☐ Aucun montage `hostPath` sauf justification documentée
- ☐ Aucun usage de `hostNetwork`, `hostPID`, `hostIPC`
- ☐ Pull policy = `IfNotPresent` ou `Always` avec `imagePullSecrets`
- ☐ Aucune image taguée `:latest` en production
- ☐ `seccompProfile.type: RuntimeDefault` sur les pods sensibles

2. RBAC, IDENTITÉS & SECRETS

- ☐ Aucune `ClusterRoleBinding` sur le ServiceAccount `default`
- ☐ Pas de wildcard `"*"` dans `verbs` ou `resources` des Roles
- ☐ RoleBindings limités au namespace cible (pas de cross-namespace implicite)
- ☐ `automountServiceAccountToken: false` par défaut, opt-in explicite
- ☐ Secrets chiffrés au repos (KMS provider configuré dans `EncryptionConfig`)
- ☐ Aucun secret en clair dans les manifests, ConfigMaps ou variables d'env
- ☐ Rotation des certificats kubelet et API server documentée et automatisée
- ☐ External Secrets Operator ou équivalent pour les credentials longue durée

3. RÉSEAU, ADMISSION & APPROVISIONNEMENT

- ☐ NetworkPolicy par défaut `default-deny` sur chaque namespace applicatif
- ☐ Webhooks d'admission validés (`failurePolicy` explicite, jamais `Ignore` en prod)
- ☐ Kyverno (ou équivalent) en mode `enforce` sur les policies critiques
- ☐ Image scan obligatoire avant push registry (Trivy / Grype / Clair)
- ☐ Signature d'images avec Cosign + vérification au pull (Kyverno verifyImages)
- ☐ Resource `requests` et `limits` définis sur tous les conteneurs
- ☐ LimitRange + ResourceQuota par namespace pour prévenir le bruit de voisinage

4. AUDIT, CONFORMITÉ & RÉVERSIBILITÉ

- ☐ Audit log API server activé (`--audit-policy-file`) et exporté
- ☐ Logs centralisés > 1 an (NIS2, SecNumCloud)

- ☐ Inventaire à jour : référentiel CIS K8s appliqué + delta documenté
- ☐ Plan de continuité testé : restore etcd + redéploiement complet sous 4h
- ☐ Procédure de désinstallation documentée et testée (sortie sans dépendance)

Aegis Vetis automatise tous ces contrôles.
Demander une démo : **aegis-vetis.io/contact**
Questions : hello@aegis-vetis.io

ADRIEN VINET CONSULTING SASU
14 rue Bausset, 75015 Paris · SIRET 982 646 556 00018
Mentions légales : aegis-vetis.io/legal