Detect Abuse of Container APIs for Credential Access, Detection Strategy DET0198

Archived: 2026-04-05 16:25:34 UTC

AN0571

Detection correlates anomalous Docker or Kubernetes API requests with access to logs, secrets, or service accounts. Observes unauthorized use of `docker logs`, `kubectl get secrets`, or direct API calls to Kubernetes API server endpoints. Identifies behavioral patterns where adversaries escalate from basic pod/container interaction to privileged API calls exposing sensitive credential material.

Log Sources

Mutable Elements

Field	Description
UserContext	Tune to exclude known orchestrator admin service accounts or CI/CD pipelines that legitimately access secrets
NamespaceScope	Restrict detection to sensitive namespaces (e.g., kube-system, production apps)
TimeWindow	Adjust correlation timing between pod execution and subsequent API secret retrieval
SourceIP	Filter based on allowed internal API calls vs anomalous external or cross-cluster access

---