Detection Strategy for Container and Resource Discovery, Detection Strategy DET0490

Archived: 2026-04-05 17:24:22 UTC

AN1352

Detection of adversary attempts to enumerate containers, pods, nodes, and related resources within containerized environments. Defenders may observe anomalous API calls to Docker or Kubernetes (e.g., 'docker ps', 'kubectl get pods', 'kubectl get nodes'), unusual account activity against the Kubernetes dashboard, or unexpected queries against container metadata endpoints. These events should be correlated with user context and network activity to reveal resource discovery attempts.

Log Sources

Mutable Elements

Field	Description
UserAllowList	Defines which service accounts and admin roles are expected to perform discovery actions. Activity by non-allowlisted identities may indicate adversary discovery.
TimeWindow	Specifies correlation period (e.g., 10m) for linking multiple discovery attempts across API and daemon logs.
PodQueryThreshold	Defines threshold for number of pod/node enumeration requests by a single user. Excessive queries may indicate scanning activity.
