Detection Strategy for Container Administration Command Abuse, Detection Strategy DET0065

Archived: 2026-04-05 15:43:13 UTC

AN0177

Defenders may detect abuse of container administration commands by observing anomalous use of management utilities (`docker exec` , `kubectl exec` , or API calls to kubelet) correlated with unexpected process creation inside containers. Behavioral chains include unauthorized API requests followed by command execution within running pods or containers, often originating from unusual user accounts, automation scripts, or IP addresses outside the expected cluster management plane.

Log Sources

Mutable Elements

Field	Description
AuthorizedAdminUsers	Expected admin accounts allowed to use exec commands; anomalies outside this list indicate possible abuse.
ExecFrequencyThreshold	Defines how often `docker exec` or `kubectl exec` is normally observed; sudden spikes may indicate adversary behavior.
SourceIPRange	Expected IP ranges for management actions (e.g., cluster control plane). Requests from external/unexpected ranges may indicate compromise.
NamespaceScope	Defines which namespaces typically allow exec operations; anomalous activity outside these may indicate lateral movement.