Detect persistent or elevated container services via container runtime or cluster manipulation, Detection Strategy DET0473

Archived: 2026-04-05 16:55:24 UTC

Analytics

- Containers

AN1304

Correlate the creation or modification of containers using restart policies (e.g., 'always') or DaemonSets with elevated host access, service account misuse, or privileged container contexts. Watch for manipulation of systemd units involving containers or pod scheduling targeting specific nodes or namespaces.

Log Sources

Mutable Elements

Field	Description
restartPolicy	Tune for environments that legitimately use 'always' or 'unless-stopped' in trusted containers
targetNamespace	Scope detection to high-risk namespaces (e.g., kube-system)
nodeSelector|nodeName	Adjust if targeting known cluster configurations or test environments
unitFilePath	Adapt to your OS/systemd hierarchy and container binary references
TimeWindow	Adjust temporal correlation (e.g., container launch → privilege escalation)
