Detection Strategy for Masquerading via Legitimate Resource Name or Location, Detection Strategy DET0347

Archived: 2026-04-05 12:56:42 UTC

AN0983

Detects processes or binaries executed from trusted directories (e.g., System32) or using trusted names (e.g., svchost.exe) where the metadata, hash, or parent process does not align with legitimate activity patterns.

Log Sources

Mutable Elements

Field	Description
trusted_directory_list	Paths such as C:\Windows\System32 that adversaries may abuse
process_baseline_age	Time window to determine process novelty (e.g., 30 days)

AN0984

Detects renamed binaries or scripts placed into trusted paths like /usr/bin or /lib with mismatched metadata or unexpected creation/modification times.

Log Sources

Mutable Elements

Field	Description
monitored_paths	Set of system or application directories considered sensitive or trusted
hash_validation_window	Timeframe during which a newly created file should have its hash validated (e.g., within 5 minutes of write)

AN0985

Detects binaries or launch daemons in /System/Library or /Applications with mismatched bundle names, unexpected metadata, or improper installation origin.

Log Sources

Mutable Elements

Field	Description
expected_bundle_names	List of known application names and paths to validate against
signed_by_apple_check	Toggle to enforce checks for Apple-signed binaries in trusted directories

AN0986

Detects malicious containers or pods using names, labels, or namespaces that mimic legitimate workloads; also checks for image layer mismatches and unauthorized resource deployments.

Log Sources

Mutable Elements

Field	Description
trusted_namespace_list	List of namespaces that should not be used by unprivileged users or workloads
image_baseline_hashes	Reference hashes of approved container images

AN0987

Detects VIBs, scripts, or binaries placed into directories like /bin or /etc/vmware with names mimicking standard ESXi components. Also monitors unauthorized creation of services.

Log Sources

Mutable Elements

Field	Description
esxi_baseline_file_list	Known good binaries and their expected paths
service_creation_alert_threshold	Threshold for unknown service names or mismatched digital signatures

---