Detection Strategy for Abuse Elevation Control Mechanism (T1548), Detection Strategy DET0345

Archived: 2026-04-05 13:25:48 UTC

AN0975

Correlate registry modifications (e.g., UAC bypass registry keys), unusual parent-child process relationships (e.g., control.exe spawning cmd.exe), and unsigned elevated process executions with non-standard tokens or elevation flags.

Log Sources

Mutable Elements

Field	Description
ElevatedProcessPath	Paths to monitor for unsigned or unexpected elevated binaries
ParentProcessName	Parent-child execution chains that are suspicious in the local environment
TimeWindow	Time between registry modification and elevated process spawn

AN0976

Monitor audit logs for setuid/setgid bit changes, executions where UID ≠ EUID (indicative of sudo or privilege escalation), and high-integrity binaries launched by unprivileged users.

Log Sources

Mutable Elements

Field	Description
WatchedDirectories	Paths where unauthorized setuid binaries may be dropped
UserContext	Which users are allowed to run sudo/pkexec or modify binaries
TimeWindow	Duration between file permission change and elevated command execution

AN0977

Detect execution of `/usr/libexec/security_authtrampoline` or use of AuthorizationExecuteWithPrivileges API, and monitor process lineage for unusual launches of GUI apps with escalated privileges.

Log Sources

Mutable Elements

Field	Description
WatchedBinaries	Specify binaries frequently targeted for privilege escalation
ExecutionParent	Which applications should never be allowed to spawn elevated processes

AN0978

Monitor for unexpected privilege elevation operations via SAML assertion manipulation, role injection, or changes to identity mappings that result in access escalation.

Log Sources

Mutable Elements

Field	Description
AuthorizedRoleMappings	Roles or groups that should never be assumed outside designated paths
TimeWindow	Time between assertion issuance and critical privilege use

AN0979

Detect sudden privilege escalations such as IAM role changes, user-assigned privilege boundaries, or elevation via assumed roles beyond normal behavior.

Log Sources

Mutable Elements

Field	Description
PermittedRoleTransitions	Define valid transitions between IAM roles
CrossAccountBoundary	Should flag if assumption crosses trust boundary

---