Detection of Adversary Abuse of Software Deployment Tools, Detection Strategy DET0223

Archived: 2026-04-05 13:59:24 UTC

AN0623

Detects SCCM, Intune, or remote push execution spawning scripts or binaries from SYSTEM context or unusual consoles (e.g., cmtrace.exe launching PowerShell or cmd.exe).

Log Sources

Mutable Elements

Field	Description
ParentImageList	Allowlist of known SCCM-related binary spawners (e.g., 'CCMExec.exe')
UserContext	Expected deployment activity from scheduled system accounts
TimeWindow	Unusual deployment timing outside standard maintenance hours

AN0624

Detects remote scripts or binaries deployed via Puppet, Chef, Ansible, or shell scripts from orchestration servers executing outside maintenance windows or in unmanaged nodes.

Log Sources

Mutable Elements

Field	Description
DeployingHostAllowList	Approved orchestration or jump box IPs
ScriptExecutionBaseline	Expected scripts, interpreters, or package managers used

AN0625

Detects script or binary execution initiated via JAMF, Munki, or custom MDM agents outside of baseline, or JAMF launching new Terminal or osascript processes from remote command payloads.

Log Sources

Mutable Elements

Field	Description
SigningAuthorityList	Expected signing authorities for JAMF and MDM scripts
RemoteCommandInterval	Frequency of remote execution from MDM servers

AN0626

Detects cloud-native software deployment or management (e.g., SSM Run Command, Intune) initiating script execution on endpoints outside expected org IDs, admin groups, or maintenance windows.

Log Sources

Mutable Elements

Field	Description
IAMRoleAllowList	Approved deployment administrators or service accounts
ExecutionTargetList	Expected endpoints targeted by SaaS deployments

AN0627

Detects central router or switch config management tools (e.g., FortiManager, Cisco Prime) triggering device reboots or config pushes using abnormal accounts or IPs.

Log Sources

Mutable Elements

Field	Description
PushSourceAllowList	Devices or IPs allowed to push firmware or scripts
AuthUserPattern	Expected CLI or API user performing configuration

---