Detection Strategy for Lateral Tool Transfer across OS platforms, Detection Strategy DET0183

Archived: 2026-04-05 17:09:53 UTC

AN0516

Correlate suspicious file transfers over SMB or Admin$ shares with process creation events (e.g., cmd.exe, powershell.exe, certutil.exe) that do not align with normal administrative behavior. Detect remote file writes followed by execution of transferred binaries.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Time period between file transfer and execution used to correlate events
UserContext	Accounts allowed to perform legitimate administrative transfers
FilePathWhitelist	Exclude known legitimate software update directories

AN0517

Monitor scp, rsync, curl, sftp, or ftp processes initiating transfers to internal systems combined with file creation events in unusual directories. Correlate transfer activity with subsequent execution of those binaries.

Log Sources

Mutable Elements

Field	Description
AllowedTools	Define legitimate transfer utilities expected in the environment
DestinationDirectories	Restrict to suspicious or non-standard directories for transferred files

AN0518

Detect anomalous use of scp, rsync, curl, or third-party sync apps transferring executables into user directories. Correlate new file creation with immediate execution events.

Log Sources

Mutable Elements

Field	Description
SyncApplications	Whitelisted apps like Dropbox or OneDrive if sanctioned
EntropyThreshold	Adjust threshold for unusual filenames/hashes transferred internally

AN0519

Identify lateral transfer via datastore file uploads or internal scp/ssh sessions that result in new VMX/VMDK or script files. Correlate transfer with VM execution or datastore modification.

Log Sources

Mutable Elements

Field	Description
DatastoreWhitelist	Known authorized paths for legitimate VM operations
TransferProtocol	Protocols allowed for intra-VM host transfers

---