Detection Strategy for Data from Network Shared Drive, Detection Strategy DET0410

Archived: 2026-04-05 14:37:13 UTC

AN1145

Monitoring of file access to network shares (e.g., C$, Admin$) followed by unusual read or copy operations by processes not typically associated with such activity (e.g., PowerShell, certutil).

Log Sources

Mutable Elements

Field	Description
ShareName	Organizations may use custom share paths outside of default C$, Admin$, etc.
ProcessName	Common toolsets vary; defenders should tailor to unusual processes for their environment.
TimeWindow	Time of day and access duration may need to be tuned to reduce false positives.

AN1146

Unusual access or copying of files from mounted network drives (e.g., NFS, CIFS/SMB) by user shells or scripts followed by large data transfer.

Log Sources

Mutable Elements

Field	Description
MountPoint	Organization-specific share mount paths may vary (/mnt/share1, /srv/data etc.)
UID	May need to scope to service accounts or user ID patterns specific to enterprise policy.

AN1147

Detection of file access from mounted SMB shares followed by copy or exfil commands from Terminal or script interpreter processes.

Log Sources

Mutable Elements

Field	Description
ProcessPath	Script interpreters may vary (e.g., zsh, bash, python, osascript).
SharePath	Network drive mount points may differ across enterprises.
