Detection of USB-Based Data Exfiltration, Detection Strategy DET0220

Archived: 2026-04-05 18:40:47 UTC

Analytics

- Windows
- Linux
- macOS

AN0616

Detects USB device insertion followed by high-volume or sensitive file access and staging activity by suspicious processes or accounts.

Log Sources

Mutable Elements

Field	Description
SensitiveFilePathRegex	Match data staging or export paths (e.g., *.docx, *.csv, *.db) to USB volume letters.
UserContext	Limit to users who do not normally use removable devices (e.g., service accounts).
TimeWindow	Correlate events within a short period following USB insert (e.g., 5–10 minutes).

AN0617

Detects USB block device mount followed by file access in sensitive directories or high-volume copy operations by user-controlled processes.

Log Sources

Mutable Elements

Field	Description
MountPath	Look for /media/, /mnt/, /run/media/ paths associated with removable storage.
CopyCommandSignature	Detect rsync, cp, tar, zip activity writing to USB mount point.

Field	Description
AccessRateThreshold	Define abnormal access patterns (e.g., >100 files in <5 min).

AN0618

Detects external volume mount with Finder, Terminal, or script-initiated file copy from user profiles, sensitive folders, or cloud storage sync directories to USB.

Log Sources

Mutable Elements

Field	Description
DriveLabelFilter	Flag removable volumes with suspicious or default names (e.g., NO NAME, BACKUP_01).
ScriptExecutionContext	Watch for shell or AppleScript execution tied to USB copy.
VolumeMountFrequency	Detect repeated or abnormal device mounts during work hours.
