Abuse of Information Repositories for Data Collection, Detection Strategy DET0413

Archived: 2026-04-05 12:49:49 UTC

AN1160

Programmatic or excessive access to file shares, SharePoint, or database repositories by users not typically interacting with them. This includes abnormal access by privileged accounts, enumeration of large numbers of files, or downloads of sensitive content in bursts.

Log Sources

Mutable Elements

Field	Description
UserContext	Privileged users may be excluded if they routinely perform admin actions on SharePoint or file shares.
AccessVolumeThreshold	The number of files accessed or pages retrieved in a short window to flag as abnormal.
TimeWindow	The time range (e.g., 5 minutes, 1 hour) in which burst access patterns are considered anomalous.

AN1161

Command-line tools (e.g., curl, rsync, wget, or custom Python scripts) used to scrape documentation systems or internal REST APIs. Unusual access patterns to knowledge base folders or shared team drives.

Log Sources

Mutable Elements

Field	Description
CommandRegex	Regex matching internal doc servers, knowledge base paths, or IP patterns.
TimeWindow	Burst access of repositories over a short time window.

AN1162

Abuse of SaaS platforms such as Confluence, GitHub, SharePoint Online, or Slack to access excessive internal documentation or export source code/data. Includes use of tokens or browser automation from unapproved IPs.

Log Sources

Mutable Elements

Field	Description
APIUsageThreshold	Number of API calls or files accessed before triggering detection.
KnownSafeIPs	Whitelist of internal IPs/users that may be excluded from detection.

AN1163

Access of mounted cloud shares or document repositories via browser, terminal, or Finder by users not typically interacting with those resources. Includes script-based enumeration or mass download.

Log Sources

Mutable Elements

Field	Description
AccessedMountPath	Paths to sensitive volumes may differ based on org setup.
UserGroup	Expected user groups that typically access shared data.
