BENIGN 94/100

Bulk Drive download by user4@example.com is offboarding-related personal-work archiving on his last week, matching HR ticket HR-2841 - own drafts and moodboards only, corporate device, no external sharing; proceed with standard offboarding.

HOST Google Drive (cloud) USER **user4@example.com** TIME **2026-07-09T09:52:18Z**

MITRE **T1530 (Data from Cloud Storage - ruled out), T1567 (Exfiltration Over Web Service - ruled out)**

SEVERITY MEDIUM

Org: ORG001 · Alert ORG001-GOOGLE-2 · Generated 2026-07-09T10:31:44Z

EXECUTIVE SUMMARY

The "Bulk file downloads from Drive" alert on `user4@example.com` (Marcus, Design) is a false positive driven by expected offboarding behavior. Marcus's last working day is Friday 2026-07-10 per HR ticket `HR-2841`, and this morning he downloaded 312 files (~4.1 GB) over a 47-minute window - 97% of them files he created and owns, consisting of design drafts, moodboards, and personal working files. The download occurred on his managed corporate laptop from the office egress IP, involved no files carrying the org's `Confidential` or `Restricted` Drive labels, and was accompanied by zero external-sharing, forwarding, or personal-account transfer events. Manager-approved archiving of personal work product is permitted by the offboarding policy, and the HR ticket's offboarding checklist explicitly includes this step. No action is required on the alert; standard offboarding (Friday suspension and ownership transfer) should proceed, with a routine DLP verification of the downloaded set as a belt-and-braces check.

ALERT DETAILS

CREATED AT	2026-07-09T09:52:18Z
HOST	Google Drive (cloud); download client: Drive web on managed Chrome, device `MBP-DES-0244`
USER	`user4@example.com` (Marcus V., Design; offboarding, last day 2026-07-10)
SEVERITY	MEDIUM
MITRE	T1530 (Data from Cloud Storage - ruled out), T1567 (Exfiltration Over Web Service - ruled out)
PATTERN	312 file downloads (~4.1 GB) in 47 minutes, exceeding the 100-file/hour rule threshold
FILES	303 owned/created by the user (design drafts, moodboards, personal working docs); 9 shared-with-user files, none label-restricted
SOURCE IP	`203.0.113.24` (office egress range, Manchester HQ)

BUSINESS CONTEXT	HR ticket `HR-2841` (offboarding, opened 2026-06-30); checklist step "archive personal work product" approved by manager 2026-07-07
PRIOR CASES	No prior cases for this user; 4 prior org cases of the same rule firing on offboarding users, all benign (most recent ORG001-GOOGLE-1 rule-tuning recommendation still open)

INVESTIGATION QUESTIONS

What was downloaded, and does the user own it?

• The set is overwhelmingly the user's own work product: 303 of 312 files were created and are owned by him, none carry restricted Drive labels, and the 9 shared files are collaborative design assets he co-authored.

- Drive audit log enumerates 312 `download` events, 09:03-09:50Z; 303 files have `owner=user4@example.com`
- File types are design working files: Figma exports, PNG/PSD moodboards, draft decks, and personal notes docs
- Zero files carry the org's `Confidential` or `Restricted` Drive labels; DLP label scan of the file ID set returned no matches
- The 9 non-owned files are shared design-team assets on which the user is a listed collaborator with edit history
- No downloads touched Finance, HR, Legal, or customer-data shared drives; activity stayed within the user's My Drive and the Design team drive

▸ How we got the answer (2 data points)

Is there a legitimate business context that explains the burst?

• The download matches an approved offboarding checklist step: HR ticket HR-2841 sets the user's last day as Friday, and his manager approved personal-work archiving two days ago.

- HR ticket `HR-2841` (opened 2026-06-30) records resignation with last working day 2026-07-10
- The ticket's offboarding checklist includes "archive personal work product (manager approval required)" - approved by the design manager on 2026-07-07
- Timing fits the pattern: archiving performed the Wednesday before a Friday departure, during working hours
- The user's calendar shows offboarding-related meetings this week (handover sessions, exit interview scheduled Friday)
- This is the 5th occurrence of this rule firing on an offboarding user in the org; all 4 prior cases were benign with the same HR-ticket correlation

▸ How we got the answer (2 data points)

Are there any exfiltration indicators - external sharing, personal-account transfer, or anomalous device and location?

- **None: the activity came from his managed corporate laptop on office egress, with zero external shares, no transfers to personal accounts, no Takeout export, and no forwarding rules.**

- Device `MBP-DES-0244` is the user's assigned managed laptop; endpoint verification passed and session is the established corporate profile
- Source IP `203.0.113.24` is Manchester HQ office egress - the user's badge shows on-site today
- Zero `change_user_access`, `change_document_visibility`, or share-to-external events by the user in the trailing 14 days
- No Google Takeout export was initiated, no files were shared or transferred to non-domain accounts, and no mail forwarding rules exist on the mailbox
- Login history for the trailing 7 days shows only the corporate device from office and home IPs, all with 2SV satisfied and `is_suspicious: false`

▸ How we got the answer (3 data points)

CONCLUSION

This alert is a false positive. The bulk-download rule fired on volume alone, but every contextual signal aligns with sanctioned offboarding behavior: the user departs Friday under HR ticket `HR-2841`, his manager approved personal-work archiving two days before the download, the file set is 97% self-owned design work with zero restricted labels, and the session came from his managed device on office egress with no external sharing, Takeout, or transfer activity anywhere in the trailing window. This is also the fifth benign firing of this rule on a departing employee, reinforcing the open recommendation to correlate the rule with HR offboarding status. Standard offboarding should proceed as planned, with a routine DLP confirmation on the downloaded set for completeness.

RECOMMENDED ACTIONS

RECOMMENDED

1 MEDIUM **Correlate the bulk-download rule with HR offboarding status** - This is the 5th benign firing on a departing employee. Enrich the rule with HR-ticket lookup so downloads by users with an approved offboarding checklist route to auto-triage with an audit note, while non-offboarding bursts keep full severity.

2 LOW **Complete standard offboarding controls on Friday** - Suspend the account at end of day 2026-07-10, transfer Drive ownership to the design manager, wipe corporate data from the managed device, and revoke active sessions per the offboarding runbook.

3 LOW **Archive the DLP verification with the HR ticket** - Attach the label/content scan result for the 312-file set to HR-2841 so the departure record shows the archive was verified clean at the time of download.

Activity Timeline

2026-06-30	HR ticket HR-2841 opened: resignation recorded for user4@example.com, last working day 2026-07-10
2026-07-07	Design manager approves offboarding checklist step "archive personal work product"
2026-07-09T08:41:07Z	User signs in on managed device MBP-DES-0244 from Manchester HQ egress; 2SV satisfied, is_suspicious: false
2026-07-09T09:03-09:50Z	312 Drive downloads (~4.1 GB): 303 self-owned design files, 9 co-authored team assets; no restricted labels
2026-07-09T09:52:18Z	Bulk-download rule threshold (100 files/hour) exceeded - alert triggered
2026-07-09T10:20Z	Sharing/Takeout/forwarding sweep and DLP label scan complete: no exfiltration indicators, no restricted content