BENIGN 93/100

False positive: HR user user1@example.com shared interview feedback docs to domain-internal link — recurring workflow, not external exposure.

HOST `Google Drive (cloud)` USER `user1@example.com` TIME `2026-06-03T06:54:27Z`

MITRE `T1567 — Exfiltration Over Web Service (ruled out)` SEVERITY `LOW`

Org: ORG001 · Alert ORG001-GOOGLE-1 · Generated 2026-06-03T17:28:08Z

EXECUTIVE SUMMARY

The "File Shared Externally" alert is a false positive caused by the rule misclassifying `people_within_domain_with_link` sharing as external. The actor, `user1@example.com`, is an HR/operations user who changed four "Interview Feedback" Google Docs from private to domain-link visibility — a sharing scope accessible only to `example.com` users. This is the second occurrence of an identical two-step recruiting workflow within 7 days (resume PDFs shared one day, corresponding interview feedback docs shared the next), with no external recipients involved. No action is required on this alert; the rule definition should be reviewed to exclude domain-scoped link sharing.

ALERT DETAILS

ALERT ID	ORG001-GOOGLE-1 (00000000-0000-0000-0000-000000000001)
ALERT TYPE	Activity Rule — File Shared Externally
PROVIDER	Google Security Center
CREATED AT	2026-06-03T06:54:27Z
HOST	Google Drive (cloud)
USER	`user1@example.com`
SEVERITY	LOW
SOURCE IP	`198.51.100.23` (India/Delhi, ASN 64500 — Example ISP)
FILES AFFECTED	4 × Interview Feedback Google Docs (Candidate A, Candidate B, Candidate C, Candidate D)
VISIBILITY CHANGE	private → `people_within_domain_with_link` (example.com domain only)
MITRE	T1567 — Exfiltration Over Web Service (ruled out)

INVESTIGATION QUESTIONS

What files were shared and to whom — is this actually an external share?

No external sharing occurred — all four documents were set to domain-link visibility scoped to example.com users only.

- 4 Google Docs titled 'Interview Feedback - [Candidate Name]' changed from private to `people_within_domain_with_link`
- Sharing method is link-based, restricted to `example.com` domain — no external email recipients
- The alert rule fires on any non-private, non-internally-shared state, incorrectly classifying domain-link sharing as 'external'
- All 4 events occurred in a ~2-minute burst (06:54–06:56Z), consistent with a batch workflow action

▸ How we got the answer (1 data point)

Is this sharing behavior consistent with the user's role and established patterns?

Yes — this is the second occurrence of an identical HR recruiting workflow within 7 days.

- user1@example.com owns a corpus of HR files: hiring spreadsheets, candidate resume PDFs, interview feedback docs, salary sheets — consistent with an HR/operations role
- Identical pattern on 2026-05-28: 5 Interview Feedback docs shared to domain-link for the same candidates whose resumes were shared the prior day (2026-05-27)
- 2026-06-03 alert event mirrors this exactly: 4 Interview Feedback docs shared for candidates whose resumes were shared on 2026-06-02
- 21 total CHANGE_DOCUMENT_VISIBILITY events in the 7-day window, all setting to people_within_domain_with_link — no public or external shares
- Google's own is_suspicious flag on the login: false

▸ How we got the answer (2 data points)

Is the source IP (198.51.100.23) suspicious — VPN, proxy, or threat-actor infrastructure?

IP is an Indian ISP connection with no VPN/proxy/Tor flags; minor threat intel hits are low-confidence and consistent with shared netblock noise.

- ASN 64500 (Example ISP Pvt. Ltd.) — classified as ISP, not datacenter or hosting
- All enrichment sources (IPAPI, IPRegistry, VirusTotal RDAP) return is_vpn=false, is_proxy=false, is_tor=false, is_datacenter=false
- 2 of 91 VirusTotal engines flagged malicious (GreyNoise, SOCRadar) — consistent with netblock-level noise, not targeted threat activity; 55 engines returned harmless
- Login at 06:43:59Z (10 min before alert) from same IP — Google flagged is_suspicious: false
- User's daily IPs vary across 7 days, all India-based — dynamic ISP addressing is consistent with this pattern

▸ How we got the answer (2 data points)

CONCLUSION

This alert is a false positive. The Google Activity Rule fires on `CHANGE_DOCUMENT_VISIBILITY` events where the new state is neither `INTERNALLY_SHARED` nor `PRIVATE`, but `people_within_domain_with_link` — which restricts access to `example.com` domain users only — is

functionally internal sharing. The actor `user1@example.com` is an HR/operations user performing a documented, recurring recruiting workflow (share resume PDFs one day, share corresponding interview feedback docs the next), with the identical pattern confirmed on 2026-05-27/28. The source IP is a legitimate Indian ISP with no anonymization flags and Google's own suspicious-login detection returned false. No data was exposed externally and no follow-up action is required on this alert.

RECOMMENDED ACTIONS

RECOMMENDED

1. MEDIUM **Refine the 'File Shared Externally' rule to exclude domain-link sharing** — Update the Google Security Center Activity Rule to add a condition excluding FILE_SHARING_METHOD = PEOPLE_WITHIN_DOMAIN_WITH_LINK, or scope it to only fire when sharing reaches external domains or public (anyone with link). This will eliminate recurring false positives from legitimate internal link-sharing workflows.

2. LOW **Populate user1@example.com's directory title/department** — The user's Google Workspace profile has no department or job title set, making role-based triage harder. Adding HR/Operations metadata would speed future investigations.

Attack Timeline

2026-06-02 (prior day)	user1@example.com shares 4 candidate resume PDFs (Candidate A, Candidate C, Candidate B, Candidate D) to people_within_domain_with_link — step 1 of recruiting workflow
2026-06-03T06:43:59Z	user1@example.com logs in from 198.51.100.23 (Delhi, India) — login_success, is_suspicious: false
2026-06-03T06:54:26Z	Interview Feedback - Candidate A changed from private → people_within_domain_with_link — alert triggered
2026-06-03T06:55:22Z	Interview Feedback - Candidate B changed from private → people_within_domain_with_link
2026-06-03T06:55:57Z	Interview Feedback - Candidate C changed from private → people_within_domain_with_link
2026-06-03T06:56:34Z	Interview Feedback - Candidate D changed from private → people_within_domain_with_link

Affected Accounts

- **user1@example.com (User One)** — HR/Operations (inferred); Delegated Admin; 2SV enforced