BENIGN 94/100

Impossible-travel pair on user7@example.com is one engineer on one managed device: the London sign-in egressed through the company's London VPN gateway during a scheduled overnight DevOps latency test, confirmed in the team's Slack thread - add corporate VPN egress IPs to trusted locations to stop the recurrence.

HOST Google Workspace (cloud) USER **user7@example.com** TIME **2026-07-09T03:54:26Z**

MITRE **T1078.004 (Valid Accounts: Cloud Accounts - ruled out), T1090 (Proxy - benign corporate VPN, not anonymization)**

SEVERITY MEDIUM

Org: ORG001 · Alert ORG001-GOOGLE-3 · Generated 2026-07-09T04:58:31Z

EXECUTIVE SUMMARY

The impossible-travel alert on `user7@example.com` (DevOps, New York) is a false positive caused by corporate VPN geography, not account compromise. The two sign-ins 40 minutes apart - New York at 03:12Z and London at 03:52Z - share the same managed device ID, browser fingerprint, and 2SV-satisfied session chain. The "London" IP `203.0.113.68` is the static egress of the company's London VPN point of presence, documented in the network inventory, which the user connected to while running scheduled overnight latency tests of the EU PoP. The test window is corroborated by the `#devops-infra` Slack thread planning the run, and two teammates produced the identical NY-to-London sign-in pattern within the same hour. Post-sign-in activity is routine DevOps work with no mail-rule, recovery-info, or OAuth changes. No action is required on the account; registering corporate VPN egress IPs as trusted locations in the Workspace context-aware rules will stop this class of false positive.

ALERT DETAILS

CREATED AT	2026-07-09T03:54:26Z
HOST	Google Workspace (cloud); client: Chrome on managed device `MBP-OPS-0312`
USER	`user7@example.com` (DevOps engineer, New York)
SEVERITY	MEDIUM
MITRE	T1078.004 (Valid Accounts: Cloud Accounts - ruled out), T1090 (Proxy - benign corporate VPN, not anonymization)
PATTERN	Sign-in from New York (03:12Z) followed by sign-in from London (03:52Z) - 40 minutes apart, ~5,570 km, physically impossible travel
SIGN-IN 1	03:12:37Z from `198.51.100.44` (user's known New York residential ISP), 2SV satisfied
SIGN-IN 2	

	03:52:11Z from `203.0.113.68` (company London VPN gateway static egress, ASN 64520 - corporate), 2SV satisfied, same device ID
BUSINESS SIGNAL	Scheduled overnight latency test of the EU VPN PoP; planned in Slack `#devops-infra` thread 2026-07-08, run window 03:00-05:00Z
PRIOR CASES	No prior cases for this user; corporate-VPN-egress geography has not previously triggered this rule because EU PoP testing began this week

INVESTIGATION QUESTIONS

Are both sign-ins attributable to the same legitimate user and device?

- **Both sessions come from the same managed laptop with an unbroken session chain: identical device ID and browser fingerprint, both 2SV-satisfied, and Google's own risk assessment flagged neither login.**
  - Login audit shows the same Chrome device ID and endpoint-verification serial (`MBP-OPS-0312`, the user's assigned managed laptop) on both events
  - Both sign-ins satisfied 2SV via the user's hardware security key - a phishing-resistant factor an attacker in London could not replay
  - Google's login analysis marked both events `is_suspicious: false`; the only detection fired is the geo-velocity rule
  - The 03:52Z "London" event is a session continuation triggered by the IP change when the VPN tunnel came up, not a fresh credential entry
  - No password changes, recovery-info edits, or new-device enrollments exist on the account in the trailing 30 days

▸ How we got the answer (2 data points)

Is the London IP attacker infrastructure, or corporate egress?

- **The London IP is the company's own VPN gateway: a static corporate egress documented in the network inventory, on the company ASN, with no anonymizer or threat-intel classification.**
  - `203.0.113.68` is the static egress of the London VPN point of presence, listed in the IT network inventory and firewall objects as `vpn-lon-gw-01`
  - The IP sits on ASN 64520, the company's own allocation - not a commercial VPN, proxy, Tor, or hosting provider
  - 0/93 VirusTotal engines flag the IP; enrichment returns `is_vpn=false` (commercial), `is_datacenter=false`, no anonymizer tags
  - VPN gateway logs show the user's device establishing a tunnel to the London PoP at 03:51:48Z, 23 seconds before the flagged sign-in
  - Dozens of employee sessions egress this IP daily; it is routine corporate infrastructure that simply had not intersected this user's Workspace sessions before

▸ How we got the answer (2 data points)

Is there business context for routing through London at 3am, and did anyone else show the same pattern?

- **The overnight window was a scheduled DevOps latency test of the EU VPN PoP, planned in the team's Slack thread, and two teammates produced the identical New-York-to-London sign-in pattern within the same hour.**

- Slack `#devops-infra` thread from 2026-07-08 plans EU PoP latency testing for the 03:00-05:00Z window, naming the three engineers on the run - including this user
- Two teammates show the same geo-velocity pattern (US sign-in followed by London-egress sign-in) between 03:40Z and 04:20Z; their alerts corroborate rather than compound the finding
- The user's activity during the London session is test-consistent: infrastructure dashboards, monitoring consoles, and a latency-results spreadsheet - no mail, Drive bulk access, or admin surfaces
- No mail forwarding rules, filter changes, or OAuth consent grants were made during or after either session
- The test concluded 04:47Z; subsequent sign-ins are from the user's normal New York egress

▸ How we got the answer (3 data points)

CONCLUSION

This alert is a false positive produced by corporate VPN geography. One engineer, one managed device, one continuous 2SV-protected session chain: the "impossible" London leg is the company's own `vpn-lon-gw-01` egress, joined 23 seconds after the tunnel came up for a scheduled EU PoP latency test that was planned in Slack and mirrored by two teammates in the same hour. Hardware-key 2SV on both events rules out credential replay, and the session activity matches the test plan with no mailbox or OAuth changes. No action is needed on the account. The durable fix is configuration: register the corporate VPN egress IPs as trusted locations in the geo-velocity evaluation so PoP switching stops generating impossible-travel pairs, especially with EU PoP testing continuing this week.

RECOMMENDED ACTIONS

RECOMMENDED

1 MEDIUM **Register corporate VPN egress IPs as trusted locations for geo-velocity evaluation** - Add the documented VPN gateway egress set (including 203.0.113.68 / vpn-lon-gw-01) to the Workspace context-aware trusted-location configuration so tunnel switches between PoPs stop producing impossible-travel pairs. Two more alerts from this test series are already queued.

2 LOW **Have DevOps announce PoP test windows to the SOC** - A one-line heads-up (or a shared test calendar) for overnight egress-shifting exercises lets the queue pre-associate the window with the roster, keeping triage to seconds for the remaining EU PoP runs.

3 LOW **Close the two sibling alerts with this case as precedent** - The teammates' identical sign-in pairs from the same test window can be resolved by reference to this investigation rather than re-run in full.

Activity Timeline

2026-07-08 (prior day)	Slack #devops-infra thread schedules EU VPN PoP latency testing for 03:00-05:00Z with a three-engineer roster including user7@example.com
2026-07-09T03:12:37Z	Sign-in from 198.51.100.44 (user's known New York residential ISP) on managed device MBP-OPS-0312; 2SV satisfied via hardware security key
2026-07-09T03:51:48Z	Device establishes VPN tunnel to the London PoP (vpn-lon-gw-01) for the latency test run
2026-07-09T03:52:11Z	Workspace session re-authenticates on the new egress 203.0.113.68 (London) - same device ID, 2SV satisfied; geo-velocity pair completed
2026-07-09T03:54:26Z	Impossible-travel rule fires on the NY-London pair - alert triggered
2026-07-09T03:40-04:20Z	Two teammates on the test roster produce the identical sign-in pattern through the same London egress
2026-07-09T04:47:12Z	Test concludes; tunnel drops and the user's subsequent activity resumes from normal New York egress; results posted to the Slack thread at 04:52Z