BENIGN 93/100

Failed sign-ins on ex-employee user6@example.com are automated password-manager retries from her returned corporate laptop sitting unwiped in IT storage - zero successes against a suspended account; deactivate the account fully and wipe the device to close the noise.

HOST Okta (cloud), org example.okta.com | USER **user6@example.com** | TIME **2026-07-09T07:44:09Z**

MITRE **T1110.001 (Brute Force: Password Guessing - ruled out), T1078 (Valid Accounts - ruled out)**

SEVERITY LOW

Org: ORG001 · Alert ORG001-OKTA-2 · Generated 2026-07-09T08:27:53Z

EXECUTIVE SUMMARY

The "Repeated failed sign-ins" alert on `user6@example.com` (Priya R., departed 2026-06-19) is benign noise from incomplete offboarding, not an attack. The failures arrive every 3-4 hours in a fixed cadence from a single source: office egress IP `203.0.113.31`, with a device fingerprint and hostname matching her returned corporate laptop `LT-ENG-0187`, which MDM shows powered on in IT storage and not yet wiped. The stored browser password manager is replaying her stale credential, failing at password verification (`INVALID_CREDENTIALS`) before any MFA prompt. There are zero successful sign-ins, zero attempts against other accounts from the source, and the account has been suspended in Okta since her departure date. The residual risk is hygiene, not compromise: the account is suspended rather than deactivated and still holds 14 app assignments, and the laptop has sat unwiped for 20 days against a 5-day runbook SLA. Deactivating the account, completing deprovisioning, and wiping the device ends both the risk and the alert noise.

ALERT DETAILS

CREATED AT	2026-07-09T07:44:09Z
HOST	Okta (cloud), org `example.okta.com`
USER	`user6@example.com` (Priya R., Engineering; departed 2026-06-19; account status SUSPENDED)
SEVERITY	LOW
MITRE	T1110.001 (Brute Force: Password Guessing - ruled out), T1078 (Valid Accounts - ruled out)
PATTERN	142 failed sign-ins since 2026-06-19 at a fixed 3-4 hour cadence; single username, single source, identical user agent
FAILURE REASON	`INVALID_CREDENTIALS` on every attempt - stale password rejected before MFA; zero MFA challenges issued

SOURCE	`203.0.113.31` (office egress, Manchester HQ); device fingerprint matches returned laptop `LT-ENG-0187` (MDM: powered on, IT storage VLAN, not yet wiped)
ACCOUNT STATE	Suspended 2026-06-19 per offboarding; NOT deactivated - 14 app assignments and group memberships remain
PRIOR CASES	No prior cases for this account; same-rule noise pattern seen twice before on unwiped returned devices (both benign)

INVESTIGATION QUESTIONS

Is the failure pattern a targeted attack, credential stuffing, or automated retry?

- **The pattern is machine retry, not attack: a fixed 3-4 hour cadence from one source with one username, one identical user agent, and the same stale credential failing at password verification on every attempt.**

- 142 failures since 2026-06-19, spaced 3h12m-3h58m apart around device wake/sync cycles - no burstiness, no acceleration, no off-pattern attempts
- Every attempt targets only `user6@example.com`; the source IP has attempted no other usernames in 30 days of System Log data
- User agent is identical across all attempts (Chrome 126 on macOS with the corporate profile), consistent with a stored-credential replay rather than tooling rotation
- Failure reason is `INVALID_CREDENTIALS` at password verification on every event; no MFA challenge was ever reached and no password variations were tried
- Okta ThreatInsight raises no risk on the source, and no password-spray or credential-stuffing detections fired anywhere in the org during the window

▸ How we got the answer (2 data points)

Is the source the ex-employee's own device, or external infrastructure using her identity?

- **The source is her returned corporate laptop: the attempts come from office egress, the device fingerprint and hostname match asset LT-ENG-0187, and MDM shows that laptop powered on in IT storage, checked in but never wiped.**

- All attempts originate from `203.0.113.31`, the Manchester HQ office egress - not residential, VPN, or datacenter infrastructure
- Okta device fingerprint on the failed attempts matches the fingerprint recorded on her successful sign-ins before departure
- MDM inventory shows `LT-ENG-0187` (her assigned laptop) returned 2026-06-19, currently on the IT storage VLAN, powered on, last check-in today - wipe job never executed
- The failure timestamps align with the laptop's MDM check-in and sleep/wake cycle, matching a browser password manager retrying on network reconnect
- The runbook wipe SLA is 5 business days post-return; the device has sat unwiped for 20 days

▸ How we got the answer (2 data points)

Did any attempt succeed, and is the account otherwise exposed?

- **No attempt succeeded and the account is suspended, but offboarding is incomplete: the account was never deactivated, retains 14 app assignments, and the unwiped laptop still holds her corporate browser profile and stored credentials.**

- Zero successful sign-ins for the account since 2026-06-19 anywhere in the System Log; the suspended state would block session issuance even on a correct password
- The password was rotated to a random value during offboarding, which is why the stored credential fails - the replayed password is stale
- The account remains SUSPENDED rather than DEACTIVATED, keeping 14 app assignments and group memberships live in Okta and downstream apps
- No API tokens, active sessions, or refresh tokens exist for the account; session revocation at offboarding completed correctly
- The unwiped device retains the corporate browser profile and password-manager store - a physical-access risk while it sits in storage, independent of this alert

▸ How we got the answer (2 data points)

CONCLUSION

This alert is benign: an unwiped returned laptop is replaying a departed employee's stale password on its wake cycle, and every attempt dies at password verification against a suspended account. There is no attacker, no spraying, and no path to a session. What the alert actually surfaces is an offboarding gap - the account was suspended but never deactivated, 14 app assignments linger, and the device wipe is 15 days past SLA, leaving a corporate credential store on a powered-on machine in storage. Deactivate the account, run the wipe, and this alert stream ends permanently; correlating the failed-sign-in rule with HR departure status will keep the queue clear of the same pattern in future.

RECOMMENDED ACTIONS

MUST DO

1 MEDIUM **Deactivate user6@example.com and complete deprovisioning** - Move the account from SUSPENDED to DEACTIVATED, remove the 14 app assignments and group memberships, and confirm downstream app deprovisioning fired. This both closes the residual exposure and permanently ends the alert noise.

2 MEDIUM **Wipe LT-ENG-0187 immediately** - Execute the pending MDM wipe on the returned laptop (20 days past return, 15 past SLA), clearing the corporate browser profile and stored credentials before the device is reissued or leaves storage.

RECOMMENDED

3 MEDIUM **Audit offboarding runbook completion for recent leavers** - This is the third benign case caused by an unwiped returned device. Sweep leavers from the past 90 days for suspended-not-deactivated accounts and pending wipe jobs, and add a completion check to the runbook.

4 LOW **Correlate the failed-sign-in rule with HR departure status** - When failures target an account belonging to a departed employee and originate from a managed asset in IT custody, route to auto-triage with a deprovisioning task instead of the analyst queue.

▾ Activity Timeline

2026-06-19	Priya R.'s last working day: Okta account suspended, password rotated, sessions revoked; laptop LT-ENG-0187 returned to IT storage
2026-06-19T18:22:41Z	First failed sign-in from 203.0.113.31 with the pre-departure device fingerprint - stored credential now stale
2026-06-19 to 2026-07-09	141 further failures at a fixed 3-4 hour cadence aligned to the device's wake and network-reconnect cycle; INVALID_CREDENTIALS on every attempt, zero MFA challenges
2026-06-24	Device wipe SLA (5 business days) passes with the MDM wipe job still pending
2026-07-09T07:44:09Z	Failed-sign-in threshold rule fires - alert triggered
2026-07-09T08:15Z	Investigation confirms source is the unwiped returned laptop; account state verified suspended with zero successes; deprovisioning gaps identified