CYBERINSIGHTS TODAY · INCIDENT RESPONSE

OPTIMJACK Response Cheat Sheet

Third-party JavaScript exposure · November 16, 2026

1 · Establish exposure

□ List affected project IDs and every route that can load their scripts, including checkout, login, regional routes and cached copies.

□ Record UTC timestamps, script hashes, response headers and publishing events. Preserve suspicious files without executing them.

2 · Contain and secure publishing

□ Pause affected script delivery on sensitive routes. Verify the change from a fresh browser session.

□ Review privileged sessions and integrations. Revoke suspicious sessions and rotate implicated credentials.

3 · Assess visitor and transaction impact

□ Separate script delivery, possible access to sensitive data and confirmed loss. Record evidence gaps.

□ Check which fields were available to the page. Reconcile payment destinations against independent transaction records.

4 · Restore and verify

□ Promote a reviewed bundle and purge applicable caches. Recheck approved script and network destinations on critical routes.

□ Finish a synthetic transaction using fresh and cached sessions. Repeat after cache expiry and record who can pause delivery again.

Incident record: Route · UTC window · bundle hash · evidence owner · recovery check

Full CyberInsights investigation · Report URI evidence