02 // EXTERNAL SECURITY REVIEW

External security review: vektorcloud.example

Read-only external security check covering public web files, Certificate Transparency subdomains, DNS and email auth, HTTP security headers, and live infrastructure. Not commissioned or paid by the subject.

EXECUTIVE VERDICT AND KEY FINDINGS

- **What checks out:** Root domain serves clean TLS plus `X-Content-Type-Options`, `Frame`, and `Referrer-Policy` headers. Public dotfiles are closed.
- **What is fragile:** Two `HIGH` blockers sit open today (`F-01` ships a live Slack token inside a public `.js.map` file; `F-02` leaves `staging-api` docs and AWS RDS hostnames reachable without login) alongside 3 `MED` / 3 `LOW` gaps (DMARC `p=none` spoofing risk to your AP team, EOL Grafana `v9.5.2`, legacy domain SAN `old-northbay.example`).
- **What closing it costs:** Under 1 engineering day fixes both `HIGH` blockers (`F-01` 1h, `F-02` 0.5d). Slow pushback on a 1-hour fix is its own vendor red flag. Lower items close cleanly during a 7-30d retest.

VERDICT

CONDITIONAL

CONFIDENCE: HIGH

APEX DOMAIN	DOMAIN AGE	DNS / EDGE	MAIL / DMARC	SUBDOMAINS	FINDINGS
vektorcloud.example	2.7y (2024-02-19)	Cloudflare / Vercel	Google WS / p=none	41 (4 non-prod)	2H / 3M / 3L

SAMPLE REPORT NOTICE: Illustrative vendor case (`vektorcloud.example`, RFC 2606) matching paid Kybexo structure and public-record methodology. Prepared 2026-11-20 / Hosted copy deletes 7 days after first open; downloaded files are permanent.

01. External security overview and header matrix

01 / HEADERS AND SURFACE CHECKS

HSTS (no `includeSubDomains`)	WARN
Content-Security-Policy / Permissions	MISS
X-Content-Type / Frame / Referrer	PASS
Public configuration files	CLEAN
Public .js.map (1.42 MB)	HIGH
Unauth staging OpenAPI	HIGH
Set-Cookie (omits `HttpOnly`)	LOW
security.txt (RFC 9116)	MISS

02 / OBSERVED INFRASTRUCTURE PROFILE

DNS / EDGE	Cloudflare / Vercel / AWS ALB
MAIL / DMARC	Google WS + SendGrid / `p=none` (`~all`)
CT HOSTS	41 unique (4 non-production)
VERSION HDRS	`nginx/1.18.0` `Express`
TLS SAN NOTE	1 legacy SAN (`old-northbay.example`)
APP / AUTH	Next.js, Clerk, Stripe
ENTITY HINT	Vektor Cloud Inc.

Engineering hygiene scope: Internal code quality and generated-vs-engineered ratio cannot be assessed without repository access. Public engineering proxies observed: production source maps shipped openly, version-disclosing legacy headers (`nginx/1.18.0`), and unauthenticated staging metadata (`F-01`, `F-02`, `F-07`).

02. High-priority findings (remediate within 24 hours)

HIGH **F-01: Production source map exposes internal routes and embedded Slack token**

Production web asset / 0-24h / Vendor effort: ~1h

Observed: `https://app.vektorcloud.example/_next/static/chunks/app.8f3c1a.js.map` returns `HTTP 200` (`1.42 MB`, `application/json`). The unminified client source lists 14 undocumented internal routes and embeds a Slack bot token (`xoxb-...[REDACTED]`) in `src/lib/alerts.ts`. Disclosed free immediately under Kybexo Critical Exposure Policy.

Risk impact: Buyer risk: your customer data would sit with a vendor shipping an active internal Slack workspace token and unreleased admin routes in a public production bundle.

```
$ curl -sI https://app.vektorcloud.example/_next/static/chunks/app.8f3c1a.js.map
HTTP/2 200 | content-type: application/json | content-length: 1454080
# Embedded Slack xoxb- token confirmed in src/lib/alerts.ts (redacted)
```

Action: (1) Revoke and rotate the Slack token immediately and audit Slack logs. (2) Set `productionBrowserSourceMaps: false` in `next.config.mjs` and block `*.map` at Cloudflare WAF. (3) Move Slack alerts strictly server-side.

Source: Read-only HTTP check on `app.vektorcloud.example` (2026-11-20 UTC)

HIGH **F-02: Public staging API exposes unauthenticated OpenAPI schema and RDS metadata**

Certificate Transparency + HTTP / 0-24h / Vendor effort: ~0.5d

Observed: Certificate Transparency logs surface `staging-api.vektorcloud.example` resolving to AWS `us-east-1`. `GET /swagger.json` returns `HTTP 200` (42 routes), and `/v1/health` discloses internal AWS RDS hostname prefix (`vk-stg-pg01...rds.amazonaws.com`) and Node runtime. TLS SAN also lists `old-northbay.example`.

Risk impact: Buyer risk: non-production APIs frequently hold staging copies of customer records or relaxed auth; leaving schemas and RDS hostnames internet-facing raises operational compromise risk.

```
$ curl -sI https://staging-api.vektorcloud.example/swagger.json
HTTP/2 200 | content-type: application/json
```

Action: Gate `staging-api.vektorcloud.example` behind SSO/VPN or IP allowlisting, disable Swagger UI outside local dev, and strip internal metadata from health responses.

Source: crt.sh / Read-only HTTP check (2026-11-20 UTC)

03. Medium and low items (1-30 day remediation matrix)

ID	SEV	EFFORT	OBSERVED CONFIGURATION AND BUYER IMPACT	REMEDIATION AND VERIFICATION CHECK
F-03	MED	2-4w staged	DMARC `p=none`, SPF `~all` with active Google WS MX. Anyone can spoof `billing@vektorcloud.example` - exposes your AP team to fake bank-change invoices.	Verify DKIM, move DMARC to `p=quarantine` -> `p=reject`, SPF `-all`. Verify via `dig TXT`.
F-04	MED	0.5d	Public `grafana-us.vektorcloud.example` (`HTTP 200`, Grafana `v9.5.2`, EOL unpatched branch) among 4 non-prod CT hosts.	Move behind corporate SSO/VPN and upgrade Grafana to supported LTS (`11.x`). Verify `HTTP 401/403`.
F-05	MED	2h	Staging TLS certificate includes legacy domain `old-northbay.example` in SAN extension (corroborates `KX-SAMPLE-03`).	Remove legacy domain from ingress/TLS configs, reissue dedicated certs, publish DNS CAA.
F-06	LOW	1d	Root omits `Content-Security-Policy` and `Permissions-Policy`; HSTS omits `includeSubDomains`.	Deploy report-only -> enforcing CSP and enable `HSTS includeSubDomains` after staging lockdown.
F-07	LOW	1h	Version-disclosing headers (`nginx/1.18.0`, `Express`); session cookie `vk_sid` omits `HttpOnly`.	Set `server_tokens off`, disable `x-powered-by`, and add `HttpOnly` flag on `vk_sid`.
F-08	LOW	1h	`/robots.txt` lists `Disallow: /internal-billing/`; `/.well-known/security.txt` returns `HTTP 404`.	Remove internal path hints from `robots.txt` and publish an RFC 9116 `security.txt` file.

04. Method and read-only source ledger

REVIEW AREA	PUBLIC SOURCE / METHOD	MODE	SUMMARY
DNS and email auth	Public DNS-over-HTTPS (TXT, MX, NS, A)	Read-only	Google WS MX; DMARC p=none; SPF ~all
Subdomain inventory	Certificate Transparency logs (crt.sh)	Read-only	41 unique hosts; 4 non-prod; 1 legacy SAN
Public web assets	Root and app. HTML <script> + HEAD *.map	Read-only	1 exposed 1.42 MB source map (F-01)
Public config and API docs	Single GET/HEAD on public endpoints	Read-only	Root clean; staging OpenAPI open (F-02)
Headers and cookies	Single root HTTPS response inspection	Read-only	3/6 headers PASS; 2 version headers; 1 cookie flag
TLS SAN posture	Certificate Transparency SAN inspection	Read-only	1 legacy domain SAN on staging (F-05)

Method and independence: Not commissioned or paid by the subject. Observations collected strictly from public DNS, Certificate Transparency records, and ordinary unauthenticated HTTP GET/HEAD requests at browser rate. Eligible for 30-day verification retest and a signed external review letter for vendor security questionnaires (not a SOC 2 report or penetration test).