ShadowHunt Digital Exposure Report

Professional OSINT risk review by ShadowHunt (Alvey Group Ltd)

Super Deep Shadow (£49.99)

CLIENT

Alex Carter <alex.carter@example.com>

REFERENCE

FB-DEMO-20260319

GENERATED

19 Mar 2026, 20:49

IDENTIFIERS

alexdemo_88, acarter_demo, pixelalex, alex.carter@example.com

34/100

GREEN

5 checks | 2 strong | 3 possible | 0 weak | 12 enrichment rows

Super Deep Shadow complete. Optional next step: specialist audit / response playbook.

1) What we searched

- Username presence checks on key public platforms
- Basic profile discoverability checks
- Rapid risk scoring and immediate action guidance
- Expanded alias and variant checks across additional sources
- Public-index dorking checks for exposed document mentions
- Premium enrichment mode with deeper confidence validation

2) Executive summary

> Demo report for Facebook marketing preview only. All names, identifiers, and findings are fictional and included purely to demonstrate the report format and customer experience.

3) Evidence log

#	Source	Finding	Confidence	Reference
1	GitHub	Profile signal detected	High	github.com/alexdemo_88
2	X	Profile signal detected	High	x.com/alexdemo_88
3	LinkedIn	Possible profile signal	Medium	linkedin.com/in/alexdemo88
4	Web Dork • PDF	Email mention in indexed document	Low	example.org/demo/member-list.pdf
5	Forum Index	Historic alias mention	Low	forum.example.com/u/pixelalex

Enrichment: parsed_rows (demo_data_only) • 12 rows added

Showing the strongest rows in the core report for readability. Longer evidence can be added as appendix content without cramming the main pages.

4) Priority actions

- Within 24h: enable 2FA on primary accounts and email, and revoke any sessions you do not recognise.
- Within 7 days: rotate reused passwords, remove unnecessary public profile metadata, and review recovery options.
- Within 30 days: rerun the scan and confirm your exposure trend is moving down, not up.

5) Practical footprint reduction plan (2026)

1. Google yourself across name, email, phone, and usernames; set Google Alerts for new mentions.
2. Delete or deactivate unused accounts such as old socials, forums, shopping sites, and legacy apps.
3. Harden privacy settings on active platforms and reduce public profile visibility wherever possible.
4. Submit opt-outs to data-broker and people-search sites, or use a removal service such as DeleteMe, Incogni, or Optery.
5. Remove old or sensitive posts and request third-party removals where practical; use Google “Results about you” for de-indexing.
6. Clear browsing and search history routinely and reduce tracking and ad personalisation across major accounts.
7. Use compartmentalised identifiers such as email aliases and separate inboxes by purpose; prefer passkeys and strong MFA.
8. Audit phone and app permissions, disable ad tracking, and tighten location-history defaults.
9. Minimise future oversharing such as live location, travel plans, phone number, date of birth, and home details.
10. Use a password manager and breach monitoring, and regularly revoke stale third-party app connections.

Start with steps 1–4 for the biggest immediate reduction. Consistency beats perfection.

Limitations: lawful OSINT point-in-time checks; private or closed datasets may not be visible.