Fictional sample.

Every person, company, domain, account and wallet in this report is invented. It shows the format and depth of a real deliverable, abridged.

Cyber Investigation sample report

brindlecove-health.example

Regional clinic group, fictional organization

As of	2026-09-18
Handling	Confidential. For the client and the stated purpose only.
Evidence items	5

Intelligence requirement

For the clinic group's security lead: what can an outsider see of our external footprint, which assets are forgotten, and is anyone impersonating us?

Lawful purpose recorded in the case gate: Security exposure review of your own organization and its staff (security_exposure).

Scope and exclusions

In scope

- Domains and subdomains from certificate logs, DNS and web archives
- Hosting, certificates and registrant links between assets
- Mail posture: SPF, DKIM, DMARC and MTA-STS
- Reported credential exposure for the organization's domains
- Lookalike and impersonation domains

Not included

- Non-public records, bank or account data, and anything behind a login we do not lawfully hold
- Leaked credentials or breach contents: only the fact that an exposure was reported is recorded
- Locating or contacting any person, pretexting or covert approaches
- Health, religion, sexual life, ethnic origin or other protected traits

- Port scans, vulnerability scans, exploitation or any active testing
- Logging in with exposed credentials or testing whether they work

Executive intelligence assessment

Forty-one hostnames found, six not linked from any current page. One forgotten staging host still serves a login page. DMARC is set to monitor only. Exposure was reported for 12 staff accounts. Two lookalike domains were registered this year, one with a mail server.

Key findings

staging.brindlecove-health.example serves a login page on a certificate issued in 2026.

Fact | Confirmed E-Y-0001, E-Y-0002

DMARC policy is p=none, so spoofed mail is reported but not rejected.

Fact | Confirmed E-Y-0003

A breach notification service reports exposure for 12 accounts on the domain. Contents were not viewed.

Fact | Medium E-Y-0004

brindlecove-heath.example, registered 2026-06, has an MX record and may be prepared for phishing.

Assessment | Medium E-Y-0005

Chronology

Date	Event	Evidence
2026-02	Certificate issued for the staging host	E-Y-0001
2026-06	Lookalike domain registered, MX record added	E-Y-0005
2026-09	DMARC record observed at p=none	E-Y-0003

Contradictions and alternative hypotheses

The lookalike domain was registered defensively by a vendor or by the group itself.

Open. The registrant is privacy-protected; the group's IT team can confirm.

Intelligence gaps

- Internal assets and anything not visible from the internet.
- Which of the 12 exposed accounts are still active.

Analyst assessment

Take the staging host offline or behind access control, move DMARC to quarantine, reset the reported accounts, and watch the lookalike domain.

Reviewer sign-off: a real report cannot be sent until it passes the QA rules and a second person, not the analyst, signs it off. Both names and the sign-off time go on the cover. This sample carries none.

Evidence index

ID	Source	Class	Grade	Retrieved	SHA-256
E-Y-0001	Certificate transparency log entry	Aggregator	C2	2026-09-17	2e6ade3ee44c...
E-Y-0002	Page capture of the staging host	Self-published	D2	2026-09-17	d0245c6d2b46...
E-Y-0003	DNS TXT record, _dmarc	Established	B3	2026-09-17	b66e98dbded6...
E-Y-0004	Breach notification service, domain summary	Aggregator	C3	2026-09-17	ee317d2a3c45...
E-Y-0005	WHOIS and DNS records for the lookalike domain	Established	B3	2026-09-18	990cbfd33769...

Grade is the Admiralty code, set by rule: reliability A to F from the source class, credibility 1 to 6 from how many other independent sources support the same claim. Hashes in this sample are illustrative. In a real report each is the SHA-256 of the stored capture. How grading works