SHELL-AFFECT · CYBER ATTACK SURFACE PROFILE

Passive External Intelligence Assessment

ASSESSED

Northline Cyber Readiness Ltd.

northline-ready.example

REPORT
SA-CASP-SAMPLE-2026-08

DATE
2 August 2026

METHOD
Passive OSINT only

SECTOR
Cybersecurity training / readiness

EXTERNAL RISK
Critical

TOP DRIVER
Login + exposed credentials

PREPARED BY

SHELL-AFFECT
Valentin Dobrykov

Balthasarstrasse 3, 50354 Hürth, Germany
Freiberufliche IT- und Cybersecurity-Leistungen
USt-IdNr. DE323170877 · St.-Nr. 224/5055/4266

info@shell-affect.com
security@shell-affect.com
www.shell-affect.com
Product: CASP

1. Executive summary

External passive assessment of Northline Cyber Readiness Ltd.: what is publicly visible, which paths matter most, and what to remediate first.

OVERALL RISK	THIS WEEK	OPEN ACTIONS	CREDENTIALS
CRITICAL	Harden SSO	20	Exposed
SSO + staff + leaks	MFA + rotate secrets	4 urgent · 16 important	3 bound pairs found

PRIORITY FINDING

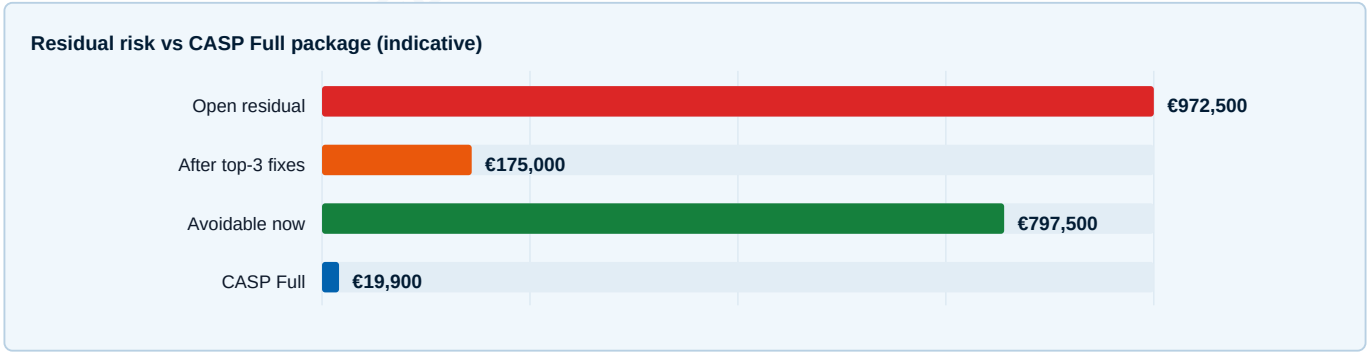
Most probable path: **public login + staff identities** (rank #1, Critical 84). Breach-corpus coverage **completed** this run: **3 email/password pairs** bound to your domain (rank #2, High 71) — reuse against SSO is the immediate stuffing risk. Next: **staging / proxy non-prod** (#3, High 74) and **mail auth short of reject** (#4, Medium 60; SPF soft-fail, DMARC quarantine). Staff emails + SSO + leaked credentials is the critical join.

1.1 Indicative residual financial risk

What leaving the open surface as-is can cost — in catalogue euros for prioritisation and ROI, not as an actuarial claim.

OPEN RESIDUAL	AFTER TOP-3 FIXES	AVOIDABLE NOW	CASP FULL
€972,500	€175,000	€797,500	€19,900

Figure F — Open residual, residual after top-3 fixes, avoidable exposure, and illustrative CASP Full package (€19,900) on one scale. The fee bar is intentionally small.



EXECUTIVE ROI SNAPSHOT

Leaving the current open findings unaddressed carries about **€972,500** in indicative open residual risk (priority-ladder catalogue euros for prioritisation — not a forecast of actual breach loss). Closing the top three paths this week (SSO MFA, leaked credentials, public non-prod) would cut that to about **€175,000** — roughly **€797,500** of avoidable exposure. Against an illustrative SHELL-AFFECT **CASP Full** package of **€19,900**, that is on the order of a **40×** residual-risk contrast for this sample (public entry: Lite from €7,500 · Full €19,900 · Re-Investigation €4,500).

Open residual by discovery

Open discovery	Pri	Risk	Indicative cost
Public SSO / login host	P0	4	€375,000

Open discovery	Pri	Risk	Indicative cost
Staff identity / mailbox corpus	P1	2	€85,000
Bound leaked credentials (3 pairs)	P0	4	€375,000
Public non-prod / staging cluster	P1	3	€85,000
Mail auth short of reject	P2	2	€15,000
Public pen-test-titled file	P2	1	€7,500
Vendor / related-domain surface	P2	2	€15,000
Technology fingerprint (advisory)	P2	2	€15,000
Total open residual			€972,500

Path-level exposure (non-additive)

Path (relative rank)	Band	Cost driver	Path cost
#1 Public login	Critical	SSO edge + staff identities (P0 × risk 4)	€125,000
#2 Credential leaks	High	3 bound email/password pairs (P0 × risk 4)	€125,000
#3 Staging systems	High	Public non-prod / proxy cluster (P1)	€85,000
#4 Email spoofing	Medium	SPF soft-fail + DMARC quarantine (P2)	€15,000
#5 Public files	Low	Pen-test-titled public file (P2 × risk 1)	€7,500
#6 Executive phishing	High	Leadership + mailbox (shares login surface)	€125,000
#7 Finance fraud	High	BEC / payment-fraud pretext (P1)	€85,000
#8 Vendor trust	High	Vendor impersonation surface (P1)	€85,000
#9 Tech fingerprint	High	Tech fingerprint / KEV advisory (P2)	€15,000

Path costs are not summed into the portfolio total — overlapping intel would double-count. Portfolio residual is the sum of distinct open discoveries above.

How these figures are calculated

Figures are **indicative residual risk costs** for prioritisation and ROI discussion — the same monetisation approach shown in the CASP platform (open residual exposure versus savings once findings are closed). They are **not** a forecast of actual loss, an insurance quote, or a regulatory fine estimate.

Calculation. Each open discovery is assigned a priority band and a risk level (1–4). Base bands follow the CASP priority ladder: P0 = €250,000 · P1 = €85,000 · P2 = €15,000. Risk scales the base: risk 4 ×1.5 · risk 2–3 ×1.0 · risk 1 ×0.5 (e.g. P0 × risk 4 = €375,000). **Portfolio residual** = sum of distinct open discoveries (items marked resolved or not applicable count as €0). **Path cost** = non-additive rollup (typically the maximum of supporting open items, so overlapping paths are not double-counted in the portfolio total). “After top-3 fixes” assumes strong multi-factor authentication cuts the login-edge cost by ~90%, and the leaked-credential and public non-production findings are closed.

Sources and calibration (not arbitrary). Two anchors set the order of magnitude: (1) **IBM Cost of a Data Breach Report** (IBM Security / Ponemon Institute methodology) — the widely cited industry study of **organisation-level average cost of a realised data breach** (multi-million EUR/USD range in recent editions; global and regional averages vary by year). CASP does **not** copy that average as residual risk; it uses it as an external ceiling/context so priority bands stay board-useful without pretending every open finding is a full breach. (2) The CASP indicative cost catalogue — about 95 threat-type entries (Company Information, Infrastructure, Leaks) with min / avg / max costs, last updated January 2026. The transparent

operational ladder **P0 €250,000 · P1 €85,000 · P2 €15,000** is a deliberate simplification of those catalogue ranges, **scaled well below** typical IBM single-breach averages because CASP prioritises **open exposures**, not a measured breach event. Same model as production assessments and open-residual tracking. Figures remain **indicative** for prioritisation — not a loss forecast, insurance quote, or actuarial model. The illustrative CASP Full package (€19,900) is a sample ROI contrast only, not a commercial quote. Public entry points: CASP Lite from €7,500; CASP Full €19,900; Re-Investigation €4,500 per run.

1.2 Method and reading guide

Collection used public sources only — no login, no authenticated testing, no origin scanning. Findings are grouped by external visibility, ranked attack path, and recommended action. Evidence is mapped to a simple six-stage attack chain (Figure A) so owners can see where public data supports recon, delivery, or exploitation.

1.3 Attack chain reference

Stages 1–4 are where passive OSINT is strongest. Stages 5–6 often need confirmation from your team (true MFA posture, payment controls, whether staging holds production data).

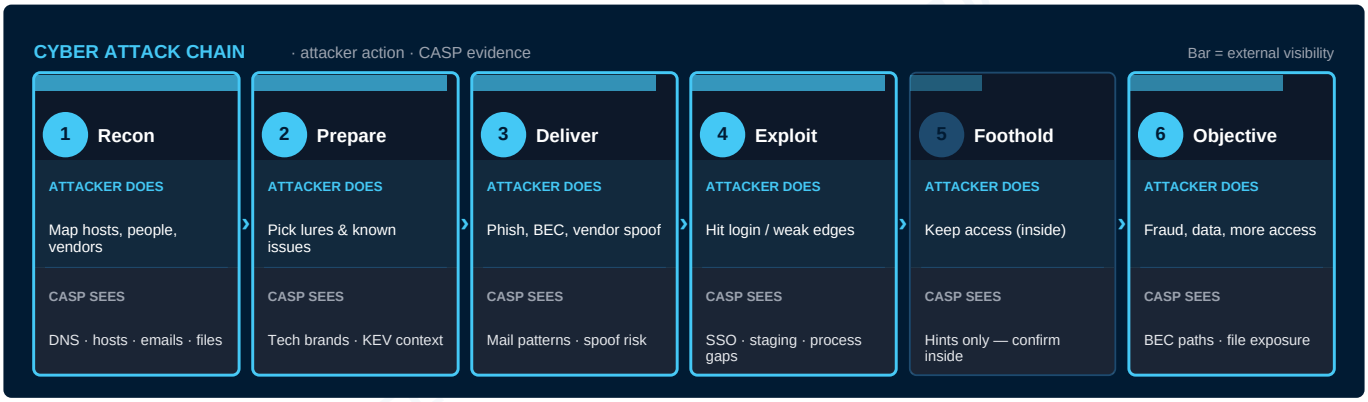


Figure A — Attack chain stages. Top bar indicates how much CASP can observe externally.

1.4 Scorecard

Topic	Result	Implication
Open residual risk	€972,500 indicative	Catalogue cost of leaving open discoveries as-is
If ranks #1–#3 closed	€175,000 residual	≈ €797,500 avoidable this week
Rank #1 path	Public login + staff identities (Critical, 84)	Path cost €375,000 · phishing / stuffing at SSO
Rank #2 path	Exposed credentials in breach data (High, 71)	Path cost €375,000 · replay at public login
Rank #3 path	Public staging / proxy non-prod (High, 74)	Path cost €85,000 · weaker edge; growing cluster
Rank #4 path	Mail auth short of reject (Medium, 60)	Path cost €15,000 · SPF soft-fail; DMARC quarantine
High score, lower rank	Tech fingerprint (High, 78) ranked #9	Stack/KEV boost ≠ confirmed self-hosted emergency
Credential coverage	Completed — 3 bound pairs (sample)	Force resets; revoke sessions; hunt reuse window
Open actions	20 (4 urgent, 16 important)	Assignable this week
Tempo	+20 hosts; 6 high-signal still open; +9 non-prod	Staging growth while prior edges age across scans
Public hosts	About 60+	Full list in technical dataset; sample in §3

1.5 Risk picture

Figure 1 — Paths by CASP score (colour = severity). Relative rank in §4 can differ from score order (see tech #8).

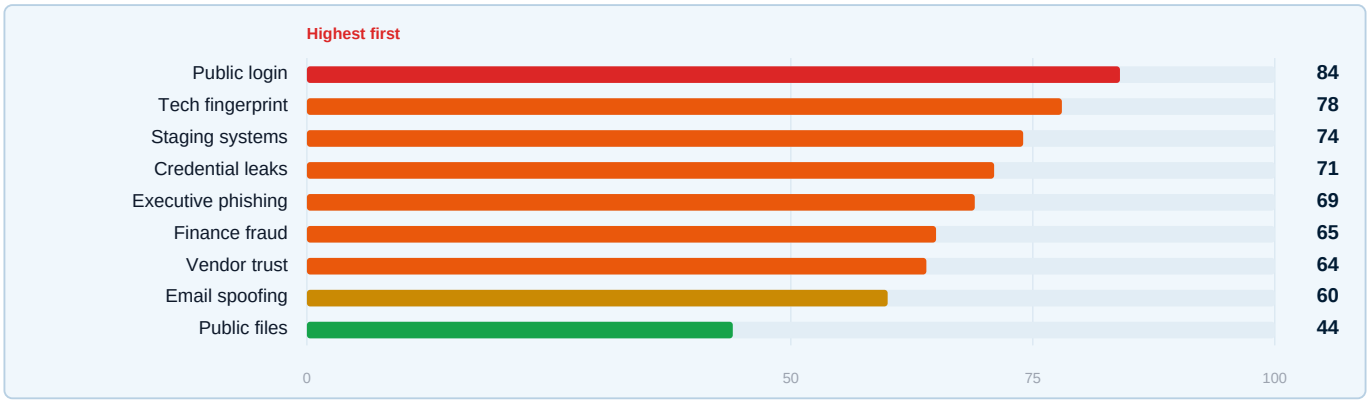
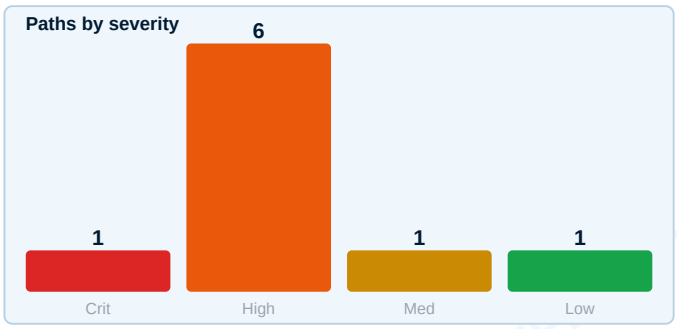
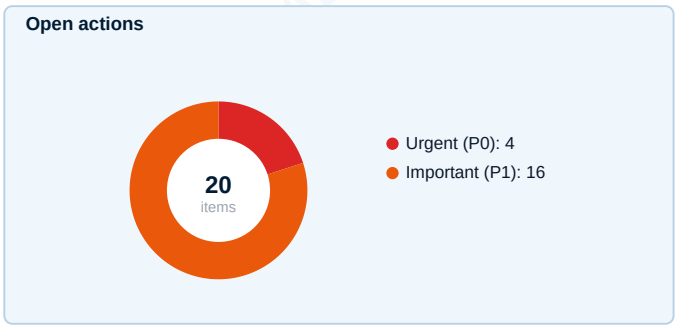


Figure 2 — Path severity (left) and open actions (right).

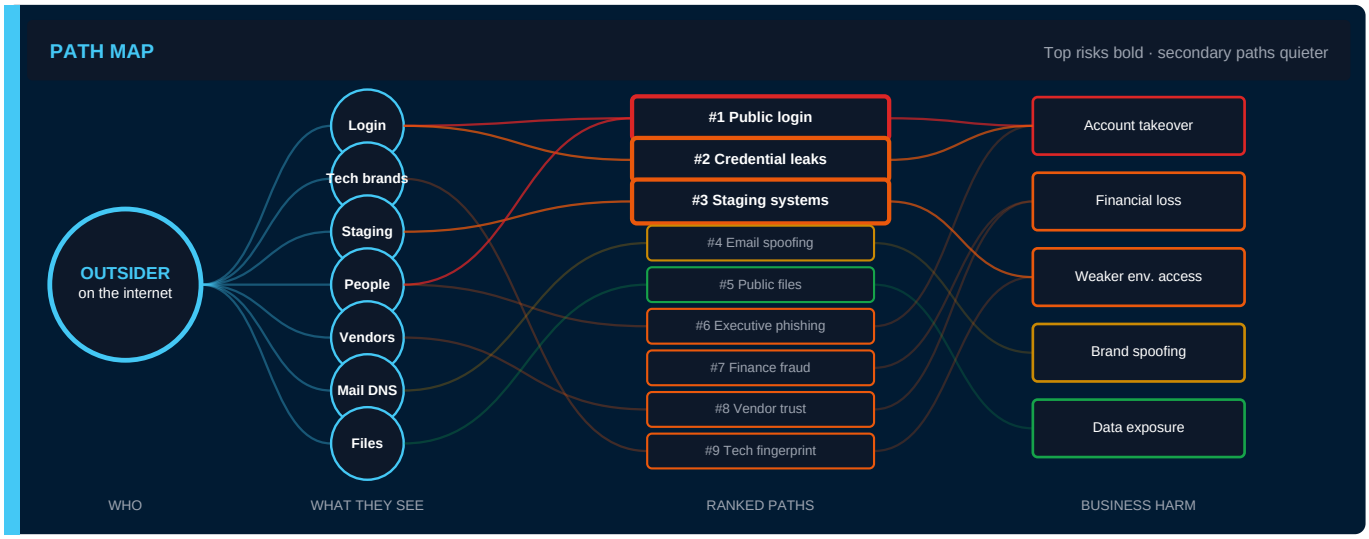




1.6 Path map

Left to right: external observer → visible assets → paths in CASP relative-rank order → impact. Top three ranks are emphasised (not always the highest raw score).

Figure 3 — Path map. Bold paths (#1–#3 by relative rank) are the priority briefing set.



1.7 Priority actions

Pri	Action	Owner	Why now
Urgent	Phishing-resistant MFA on public SSO; reduce password-only access	Identity / IT	#1 · €375,000 path cost
Urgent	Force reset + session revoke for bound leaked accounts	SecOps / Identity	#2 · €375,000; pairs at SSO
Important	Remove or protect public staging / proxy non-prod	Platform	#3 · €85,000; cluster growth
Important	Move DMARC toward reject; harden SPF/DKIM	Messaging	#4 · €15,000; SPF soft-fail
Important	Review public file titled like an internal pen-test report	Security	#5 · €7,500; confirm marketing vs real
Important	Monitor SaaS vendor KEV/advisories (e.g. collab cloud)	AppSec	KEV family hits; no version proof — advisory only

If only two items land this week: harden public SSO (#1) and rotate/reset leaked credentials (#2). Then close public non-prod (#3) and raise mail auth toward reject (#4). Together, ranks #1–#3 cut about €797,500 of indicative residual. Residual risk still depends on MFA posture, intentional demos, and payment dual-control.

2. Scope and limits

In scope: public footprint of **northline-ready.example** — hostnames, DNS, people and emails in open sources, public files, and third parties visible externally.

Out of scope: active scanning, authenticated testing, brand takedown, malware analysis, internal networks, legal advice.

Limits of this sample run:

- Credential coverage completed against public breach corpora — only bound, non-noise pairs are published.
- Exact software versions are rarely visible externally; cloud advisories are usually the vendor's job.
- Public funding or size claims are not treated as audited fact.
- Surface is a snapshot and will change.

2.1 Outside view vs inside judgment

View	Source	Answers
Outside (this report)	CASP passive collection	What is visible? Which paths rank highest?
Inside (your team)	IT, Security, Operations	Real, intentional, or already fixed?
Gap	Where those disagree	Remove, restrict, harden, or accept with note?

In the ticket system / remediation log, record an inside disposition on each item (resolved, false positive, disclosed — with a short note). This PDF freezes one sample snapshot.

3. External inventory

Representative samples for decisions. Complete host and address lists are in the technical dataset.

3.1 Themes

Theme	Scale	Stages	Implication
Public login / account hosts	SSO + account surfaces	1 · 4 · 6	Cross-module: staff emails + reachable SSO
Leaked credentials (breach corpus)	3 bound pairs (sample)	1 · 4 · 6	Reuse at SSO; force reset + session hunt
Non-production + proxy edges	Dozen+ dev/staging/proxy names	1 · 4 · 5	Cluster growth; layout leak; weaker auth
People and mailboxes	Leadership + ~10 staff samples	1 · 3 · 6	Delivery lists; BEC / spear-phish pretext
Third-party services	CDN, mail, pay, collab	1 · 2 · 3	Vendor lure names; KEV family monitoring
Public files	≥1 pen-test-titled public file	1 · 6	Title signals sensitivity; confirm if sample/marketing

3.2 Hostname sample

Hostname	Class	Stages	Implication
sso.northline-ready.example	Login	1→4	Primary auth target
account.northline-ready.example	Account	1→4	Secondary login / lifecycle surface
academy.northline-ready.example	Product	1	Product surface for recon
airflow.data-dev.northline-ready.example	Staging	1→4	Data platform; non-prod edge
analytics-dev.northline-ready.example	Staging	1→4	Non-prod analytics
app-test.northline-ready.example	Staging	1→4	Test naming signals lower controls
dbt.data-dev.northline-ready.example	Staging	1→4	Data tooling on non-prod edge
proxy.academy.northline-ready.example	Proxy / edge	1→4	Proxy naming expands edge map
proxy.ent-staging.northline-ready.example	Proxy / staging	1→4	Enterprise non-prod proxy
k8s.flock-ng-dev.northline-ready.example	k8s / staging	1	Cluster naming leaks topology
northline-solutions.example	Related domain	1→3	Related brand domain (supply / recon)
…	…	…	≈50 further hosts in full dataset

3.3 People and email sample

Identity	Context	Stages	Implication
A. Varga	CEO (public)	1→3→6	Authority pretext (BEC)
a.varga@northline-ready.example	Executive mailbox	1→3	Spear-phish delivery address
T. Fernandez	Revenue leadership (public)	1→3→6	Finance / sales pretext
s.chen@northline-ready.example	Staff sample	1→3→4	Phish list; SSO stuffing candidate
m.okonkwo@…	Staff sample	1→3→4	Phish list; SSO stuffing candidate
…	Full pack (~10 samples)	…	Further addresses expand delivery set

3.4 Credential exposure sample (breach corpus)

Subject (masked)	Type	Binding	Implication
s.chen@northline-ready.example	Email + password pair	Strong (domain match)	Replay at sso / account hosts
m.okonkwo@northline-ready.example	Email + password pair	Strong (domain match)	Replay at sso / account hosts
ops-bot@northline-ready.example	Email + password pair	Strong (domain match)	Service-style mailbox; high privilege risk if reused
Plaintext secrets not printed	Policy	—	Full digests in technical pack / remediation log only

3.5 External services

Service	Role	Stages	Implication / control
Cloudflare	DNS / edge	1	Edge posture; harden origin separately
Google Workspace	Corporate email	3→4	Delivery channel and post-phish objective
OnDMARC-class mail stack	SPF / DMARC tooling	2→3	SPF soft-fail; DMARC quarantine today
Stripe / Recurly	Payments (JS)	1→2	Payment themes in lures; inventory scripts
Atlassian Cloud	Collab SaaS	1→2	KEV family — monitor vendor (no version seen)
HubSpot	Marketing	1→2	Public scripts widen fingerprint; remove unused

4. Attack paths

Scores compare relative path strength from passive evidence. They are **not** breach probabilities. **Rank follows CASP relative rank** (how the path is prioritised for operators), not raw score alone. A high score can sit lower in rank when boosts are capped (e.g. SaaS KEV without a confirmed self-hosted version).

#	Path	Score	Severity	Stages	Impact
1	Public login and staff identities	84	Critical	1→3→4→6	Account takeover
2	Exposed credentials in public breach data	71	High	1→4→6	Account takeover
3	Public staging and test systems	74	High	1→4→5	Weaker edge access
4	Domain email spoofing risk	60	Medium	2→3	Brand spoofing
5	Public file titled like an internal pen-test report	44	Low	1→6	Data exposure
6	Executive-targeted phishing	69	High	1→3→4→6	Account takeover
7	Finance-themed payment fraud (BEC)	65	High	1→3→6	Financial loss
8	Trusted-vendor impersonation	64	High	1→3→6	Financial loss
9	Visible technology fingerprint	78	High	1→2	Targeting efficiency

Note: tech fingerprint scores **78 (High)** but ranks **#9** — stack/KEV boost with tier ceiling. Credential exposure ranks **#2** when breach-corpus coverage succeeds and pairs bind to the domain. Mail auth scores **60 (Medium)** but ranks **#4** as a practical delivery amplifier.

Detail below: ranks #1–#3 (login, leaked credentials, staging), plus mail (#4) as delivery amplifier. Tech fingerprint (#9) is high score / lower rank — see §4 table note. Other paths in §4.1.

PATH-01 · Public login and staff identities

Critical · 84

Finding

Public sign-in host **sso.northline-ready.example** is reachable. About ten staff and executive identities appear in open sources. Cross-module join: emails + SSO supports targeted phishing and credential stuffing against a real authentication edge. With completed leak coverage (PATH-02), stuffing risk is no longer theoretical. Related sample addresses: 203.0.113.10 / 203.0.113.11.

Evidence

sso.northline-ready.example; account.northline-ready.example; 203.0.113.10 / 203.0.113.11; mailboxes a.varga@northline-ready.example, s.chen@northline-ready.example (plus further samples in pack). Score note: structural 72 · corroboration 8 · sector boost.

Attack chain: 1 → 3 → 4 → 6 (account access)

Stage use of this evidence

Stage	Evidence used	Effect
1 · Recon	sso.northline-ready.example; staff names	Identifies who works here and where they authenticate
3 · Deliver	a.varga@…, s.chen@…	Phishing or password-reset lures to real people
4 · Exploit	Public SSO / password surface	Stolen, leaked, or guessed credentials; MFA fatigue if weak
6 · Objective	Session / mailbox / app access	Mail read, payments, or trusted-identity pivot

Caveat

Lower priority if the host is marketing-only, or sign-in requires phishing-resistant MFA with no password fallback.

Recommended actions

- Require phishing-resistant MFA on SSO, VPN, and mail
- Disable legacy authentication methods where possible
- Keep admin portals off the public internet or behind zero-trust access

- Reduce unnecessary public role mailboxes

PATH-02 · Exposed credentials in public breach data

High · 71

Finding

Breach-corpus coverage completed for this sample run. CASP bound **3 email/password pairs** to northline-ready.example (noise filtered; unbound or marketing hits withheld). Combined with public SSO, those secrets support credential stuffing and account takeover without phishing. Plaintext secrets are not printed in this PDF — digests live in the technical pack / remediation log.

Evidence

Subjects (masked in report): s.chen@northline-ready.example, m.okonkwo@northline-ready.example, ops-bot@northline-ready.example; reuse surface sso.northline-ready.example / account.northline-ready.example. Coverage completed for this sample run; 3 bound pairs published (noise filtered).

Attack chain: 1 → 4 → 6 (reuse → access)

Stage use of this evidence

Stage	Evidence used	Effect
1 · Recon	Breach corpus + domain binding	Confirms which org addresses appear with secrets
4 · Exploit	sso.northline-ready.example / account hosts	Replays leaked passwords or stuffing lists
5 · Foothold	Authenticated session	Session reuse if MFA weak or absent
6 · Objective	Mailbox / app / API access	Data theft, fraud, or trusted-identity pivot

Caveat

Lower priority if passwords are already rotated, accounts disabled, or pairs do not bind to live staff/service accounts.

Recommended actions

- Force password reset and revoke active sessions for affected accounts
- Check password reuse on VPN, SSO, mail, and admin tools; enable MFA everywhere
- Rotate any service-account secrets; move credentials into a vault
- Hunt for suspicious logins in the exposure window

PATH-03 · Public staging and test systems

High · 74

Finding

Multiple non-production and proxy hostnames resolve publicly under northline-ready.example (data-dev, analytics-dev, app-test, dbt, k8s-*-dev, proxy.academy, proxy.enterprise-staging). Names reveal environment layout and often sit behind weaker controls than production. Tempo: non-prod cluster growth while prior high-signal hosts remain open.

Evidence

DNS samples: airflow.data-dev.northline-ready.example, analytics-dev.northline-ready.example, app-test.northline-ready.example, dbt.data-dev.northline-ready.example, proxy.academy.northline-ready.example, k8s.flock-ng-dev.northline-ready.example (full list in dataset).

Attack chain: 1 → 4 → 5 (possible foothold)

Stage use of this evidence

Stage	Evidence used	Effect
1 · Recon	*-dev / staging / proxy / k8s names	Maps environment shape from public DNS
4 · Exploit	Public non-prod edges	Weaker auth, forgotten test accounts
5 · Foothold	Non-prod beachhead	Risk if staging trusts production (confirm inside)
6 · Objective	Data or config on staging	Customer data or secrets in non-prod

Caveat

Lower priority if staging is an intentional public demo with no path to internal systems or real customer data.

Recommended actions

- Remove public DNS or require strong auth on non-prod and proxy edges
- Ensure staging holds no production secrets or customer data
- Separate staging credentials from production
- Document intentional public demos as approved exceptions

PATH-04 · Domain email spoofing risk

Medium · 60

Finding

Mail authentication for northline-ready.example is short of a hard-fail policy. Observed posture (public DNS): **SPF soft-fail (~all)** and **DMARC quarantine at 100%** — not reject. That still eases messages that appear to come from your domain and amplifies PATH-01 / BEC / vendor fraud.

Evidence

Public DNS mail matrix: SPF soft-fail; DMARC p=quarantine pct=100; DKIM selectors not fully mapped in this sample pack.

Attack chain: 2 → 3 (amplifier for PATH-01 / BEC)

Stage use of this evidence

Stage	Evidence used	Effect
2 · Prepare	SPF soft-fail · DMARC quarantine	Checks whether the domain can be spoofed cheaply
3 · Deliver	From: looks like your domain	Higher trust for BEC and brand phish
4 · Exploit	User acts on fake internal mail	Credential harvest or payment instruction
6 · Objective	Fraud or mailbox access	Money movement or identity abuse

Caveat

Lower priority if DMARC is reject, SPF ends in -all, DKIM covers all legitimate senders, and reports are monitored.

Recommended actions

- Inventory every legitimate outbound sender
- Enable DKIM on all sending streams
- Advance DMARC from quarantine to reject
- Review DMARC aggregate reports until stable

4.1 Secondary paths

#	Path	Score	Stages	Summary	Owner
5	Pen-test-titled public file	44	1→6	Public file title suggests internal findings — confirm marketing sample vs real exposure	Security
6	Executive phishing	69	1→3→4→6	CEO + leadership mailboxes → tailored delivery → login abuse	Identity
7	Finance BEC	65	1→3→6	Public funding / finance context → fake payment instruction	Finance
8	Vendor impersonation	64	1→3→6	Visible providers + related domain → fake vendor change requests	Procurement
9	Tech fingerprint	78	1→2	High score, low rank — SaaS KEV advisory only without version proof	AppSec

Paths #6–#8 mainly **amplify PATH-01 / PATH-02** when public login, leaked secrets, and mail auth short of reject already exist. Path #5 is low score but easy to verify (URL still public?).

5. External technology exposure

Third parties visible externally — not an internal SBOM. Marketing names are not partners. Competitors alone do not justify a supply-chain path. KEV matches without observed versions are **product-family risk**, not proof of a vulnerable build.

Priority	Signal	Component	Action
Important	KEV-class family (sample CVE-2023-22527)	Collaboration SaaS (cloud)	Monitor vendor advisory; confirm tenant impact
Important	KEV-class family (sample CVE-2021-26086)	Collaboration SaaS (cloud)	Vendor monitoring — not self-hosted emergency
Important	5 KEV-linked hits · no versions observed	Atlassian-class cloud products	Honesty: SaaS → advisory only unless self-hosted proven
Important	Public payment / marketing scripts	Stripe / Recurly / HubSpot	Inventory scripts; remove unused

6. Action tracker

Urgent: ~7 days. Important: ~14 days. A-01 covers rank #1 (login). A-02 covers rank #2 (leaked credentials). A-03 covers rank #3 (non-prod). A-04 covers rank #4 (mail).

ID	Pri	Action	Owner	Due	Done when
A-01	Urgent	Harden public login (sso.northline-ready.example)	Identity	7d	Phishing-resistant MFA; legacy auth off
A-02	Urgent	Reset/rotate 3 bound leaked accounts	SecOps	7d	Resets done; sessions revoked; reuse hunt clean
A-03	Important	Remove or protect public staging / proxy	Platform	14d	No public non-prod without strong auth
A-04	Important	Mail auth toward reject (SPF/DKIM/DMARC)	Messaging	14d	DMARC reject or documented exception
A-05	Important	Review pen-test-titled public file	Security	14d	URL private/gone or accepted as public sample
A-06	Important	Vendor out-of-band + partner MFA	Procurement	14d	Process live; MFA enforced

7. Change since previous collection

Versus an earlier sample window: **+20 hosts**, including a **+9 non-prod / staging / proxy cluster** (heightened window). **6 high-signal surfaces remain open** across collections (aging exposure). Highest remaining pressure: public login (rank #1) and non-prod growth (rank #2). Score calibration also lowered several paths from earlier inflated ceilings — rank order is more stable than raw score alone.

8. Recommended next steps

Step	Who	Action
1	Security lead	Brief leadership from §1 only (~5 minutes)
2	Identity / platform	Accept or challenge A-01 and A-03 (Appendix A)
3	Item owners	Set disposition in ticket system / remediation log (Appendix B)
4	Security lead	Re-scan; confirm Appendix A completion criteria

30 / 90 DAY OUTCOMES

30 days: phishing-resistant public login, leaked accounts reset, no unnecessary public staging, mail auth moving toward reject. 90 days: aging items cleared on re-scan, vendor process documented, re-scan shows pairs gone or rotated. Operator detail: Appendices A–C.

Appendix A — Close-out checklists

Printable verification for urgent and important workstreams. Tick offline if needed, then record the matching disposition in the ticket system / remediation log (Appendix B). Action IDs match §6.

A.1 PATH-01 / A-01 — Public login · Urgent

Primary path. Pair with A-02 (leaked credentials) — same SSO surface.

	Action	Completion criteria	Verification on re-scan
☐	**Enforce phishing-resistant MFA on sso.northline-ready.example (and linked VPN / mail)**	Password-only access removed or tightly constrained	Public login requires strong MFA; legacy auth not offered
☐	**Disable legacy authentication methods on the identity edge**	No basic or legacy protocols remain enabled	Identity configuration confirms legacy methods disabled
☐	**Restrict admin portals (not world-open; prefer ZTNA or allowlist)**	Administrative interfaces are not publicly reachable without strong auth	Admin hostnames absent or access-controlled on re-scan
☐	**Reduce unnecessary public role and functional mailboxes**	Only justified public addresses remain	Staff and role-mailbox inventory shrinks on re-scan
☐	**Record disposition for related discoveries in the ticket system / remediation log**	Status set to Resolved or False positive, with a short note	Remediation log entry exists; aging high-signal items clear

A.1b PATH-02 / A-02 — Leaked credentials · Urgent

Relative rank #2 when breach-corpus coverage succeeds. Do not print plaintext passwords in tickets — use remediation-log digests.

	Action	Completion criteria	Verification on re-scan
☐	**Force password reset for bound subjects (s.chen@, m.okonkwo@, ops-bot@ on northline-ready.example)**	Resets completed; users notified out-of-band if needed	Identity system shows reset timestamps; pairs no longer valid
☐	**Revoke active sessions / refresh tokens for affected accounts**	No long-lived sessions remain from exposure window	SSO/session store purge confirmed
☐	**Hunt password reuse on VPN, mail, admin, and partner portals**	Reuse checks complete; MFA enforced where missing	Spot-check clean; remediation-log note attached
☐	**Rotate any service-account or bot credentials found in the same corpus**	ops-bot (or equivalent) secrets vaulted and rotated	Old secret disabled; monitoring shows no reuse
☐	**Record disposition for credential discoveries in the ticket system / remediation log**	Status Resolved with note after re-scan or attestation	Remediation log entry exists; aging clears

A.2 PATH-03 / A-03 — Staging, proxy, and non-production · Important

Relative rank #3. Prefer removal of public exposure over documentation alone. Includes proxy.* edges.

	Action	Completion criteria	Verification on re-scan
☐	**Remove public DNS for non-production systems, or place them behind strong authentication**	No unauthenticated public development, staging, or test edges	Hostnames no longer resolve publicly, or require SSO / VPN
☐	**Confirm staging holds no production secrets or real customer data**	Inside attestation documented by platform owner	No sensitive files or credentials bound to staging hosts
☐	**Separate staging credentials from production**	No shared production and staging secrets	Inside control confirmed; optional credential re-check if coverage available
☐	**Document intentional public demos as approved exceptions**	Exception list with owner and review date	ticket status Disclosed with exception note on those hosts
☐	**Record disposition for staging discoveries in the ticket system / remediation log**	Resolved, False positive, or Disclosed as appropriate, with a note	Remediation log updated; multi-scan delta improves

A.3 PATH-04 / A-04 — Mail authentication · Important

Relative rank #4 (Medium 60). SPF soft-fail and DMARC quarantine today — advance toward reject.

	Action	Completion criteria	Verification on re-scan
☐	**Inventory every legitimate outbound sending service**	Complete, owned list of senders for SPF	SPF includes only known legitimate senders
☐	**Enable DKIM on all sending streams**	DKIM aligned for every legitimate sender	Public DNS shows DKIM; aggregate reports remain clean
☐	**Advance DMARC from monitoring toward quarantine, then reject**	Policy at reject, or a documented time-bound exception	DMARC record and policy verified via public DNS
☐	**Review DMARC aggregate reports for at least two weeks**	No unexplained spoofing sources remain open	Inside process running; optional re-check of mail-auth posture

A.4 Remaining important actions

Complete alongside the path checklists above. Same tick / criteria / verification pattern.

	Action	Completion criteria	Verification on re-scan
☐	**A-02 — Complete leaked-account resets (see A.1b)**	All bound pairs reset; sessions revoked; reuse hunt done	Re-scan or attestation; ticket status Resolved with note
☐	**A-05 — Review pen-test-titled public file (and other sensitive titles)**	URL private/gone, or accepted as intentional public sample with note	File reclassified; ticket status Resolved, Disclosed, or False positive
☐	**A-06 — Vendor out-of-band process and partner-portal MFA**	Process is live; MFA enforced on partner portals	Inside attestation; ticket status Resolved with note
☐	**PATH-04 / tech stack — Confirm cloud vs self-hosted; track SaaS KEV advisories**	Owners named; advisory subscriptions active; no false self-hosted emergency	If SaaS-only, ticket status Disclosed with vendor-monitor note

BEFORE CLOSING AN ITEM

Confirm with inside knowledge: intentional? Already mitigated? Not your asset? Needs a ticket? Intentional public demos: mark **Disclosed** with an exception note — do not leave unmarked.

Appendix B — Disposition guide (tickets & remediation log vocabulary)

Use the same status words in tickets and in the ticket system / remediation log so outside (this report) and inside (your judgment) stay aligned. One status per discovery item; always add a short note.

Status	When to use	Who marks it	What re-scan should show
Exposed	Still public and still actionable; default open state after a scan	System (default) or operator if reopening	Item still present / still high-signal
Disclosed	Real finding but accepted/known (e.g. intentional public demo) with controls	Owner + security lead	May still appear; aging is accepted with note
Resolved	Control applied; risk closed for practical purposes	Owner; security lead verifies	Removed, hardened, or no longer meets path criteria
False positive	Not a real risk for this org (wrong bind, not owned, marketing-only host)	Owner with evidence in note	Should not drive path scores; re-scan may still list raw host if public

REMEDIATION LOG

Record each status change (who / when / why). Live state is in the remediation log; this PDF is a frozen sample. Do not mark resolved without re-scan proof or inside attestation (Appendix A).

Appendix C — Map this report to tickets & remediation log

This PDF is the offline judgment pack. The remediation log is the live workbench. Use both together.

Report section	Where to work it	Operator action
§1 Executive summary	Dashboard · Key discoveries · CASP view	Brief leadership; assign A-01 / A-03 owners
§3 External inventory	Discoveries · Infrastructure / Leaks / Company	Filter by domain; open items; set disposition
§4 Attack paths + Appendix A	CASP canvas / path detail · discovery items	Work top paths; complete Appendix A; log remediation
§6 Action tracker (A-01…A-06)	Remediation / risk performance views	Track open vs resolved; attach notes
Appendix B dispositions	Discovery status: Exposed / Disclosed / Resolved / False positive	Mark status + note; never leave silent
§7 Tempo / multi-scan	Historical scan / aging items	Confirm aging cleared after fix + re-scan

Handoff rule. If it is not in the remediation log with a disposition and note, it is not closed — even if a checkbox was ticked on paper.

Appendix D — Method and classification

Collection. Public sources only — no discovery traffic to your origins. **Scoring.** Comparative path strength from linked evidence and independent sources; weak paths cannot become Critical by accident. **Quality.** Noise held back; marketing filtered; credential pairs published only when domain-bound (this sample simulates successful breach-corpus coverage — plaintext not printed in the PDF); cloud SaaS matches treated as vendor monitoring unless self-hosted evidence appears.

Attack chain model. Stages 1–6 are a simplified operational frame for passive OSINT (not full MITRE ATT&CK; coverage).

CONFIDENTIAL · SAMPLE (ANONYMIZED) · SHELL-AFFECT — CONFIDENTIAL — For named recipients only. Do not forward without authorization. This file is an anonymized sample (fictional entity), not a live customer assessment.

Document control. SA-CASP-SAMPLE-2026-08 · 2 August 2026 · Generated 2026-08-02 · SHELL-AFFECT · CASP · Subject (sample): Northline Cyber Readiness Ltd. (northline-ready.example) · Anonymized example of official CASP structure.

End of report · SA-CASP-SAMPLE-2026-08 · SHELL-AFFECT · CASP · CONFIDENTIAL