SHELL-AFFECT · CYBER ATTACK SURFACE PROFILE

Passive externe Intelligence-Bewertung

BEWERTET

Northline Cyber Readiness Ltd.

northline-ready.example

BERICHT
SA-CASP-SAMPLE-2026-08

DATUM
2. August 2026

METHODE
Nur passives OSINT

SEKTOR
Cybersecurity-Training / Readiness

EXTERNES RISIKO
Kritisch

HAUPTTREIBER
Login + offengelegte Zugangsdaten

ERSTELLT VON

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. Zusammenfassung für die Geschäftsleitung

Passive externe Bewertung von Northline Cyber Readiness Ltd.: was öffentlich sichtbar ist, welche Pfade am wichtigsten sind und was zuerst zu beheben ist.

GESAMTRISIKO	DIESE WOCHE	OFFENE AKTIONEN	ZUGANGSDATEN
KRITISCH	SSO härten	20	Offen
SSO + Personal + Leaks	MFA + Geheimnisse rotieren	4 dringend · 16 wichtig	3 gebundene Paare

PRIORITÄRE FESTSTELLUNG

Wahrscheinlichster Pfad: **öffentliches Login und Mitarbeiteridentitäten** (Rang #1, Kritisch 84). Die Abfrage öffentlicher Leak-Datenbanken war in diesem Lauf **erfolgreich**: **3 E-Mail-/Passwort-Paare** sind an Ihre Domain gebunden (Rang #2, Hoch 71) — Wiederverwendung am SSO ist das unmittelbare Credential-Stuffing-Risiko. Danach: **öffentliche Staging- und Proxy-Systeme** (#3, Hoch 74) und **E-Mail-Authentifizierung unter Reject** (#4, Mittel 60; SPF soft-fail, DMARC quarantine). Mitarbeiter-E-Mails, SSO und geleakte Zugangsdaten bilden die kritische Verknüpfung.

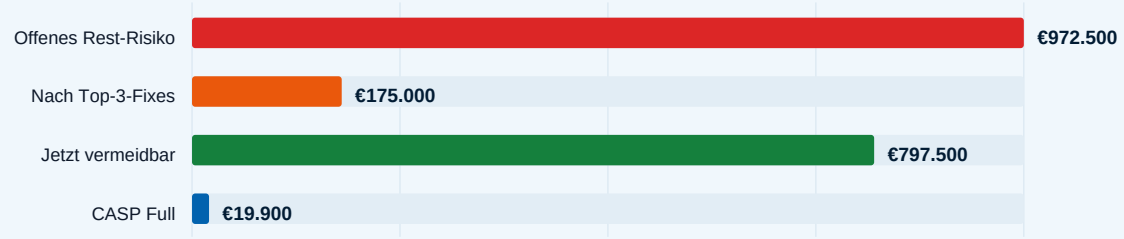
1.1 Indikatives finanzielles Rest-Risiko

Was es kosten kann, die offene Oberfläche unverändert zu lassen — in Katalog-Euro zur Priorisierung und ROI-Einschätzung, nicht als aktuarielle Schadensprognose.

OFFENES REST-RISIKO	NACH TOP-3-FIXES	JETZT VERMEIDBAR	CASP FULL
€972.500	€175.000	€797.500	€19.900

Abbildung F — Offenes Rest-Risiko, Rest nach Top-3-Fixes, vermeidbare Exposition und illustrative CASP-Jahresgebühr auf einer Skala. Der Gebührenbalken ist bewusst klein.

Rest-Risiko vs. CASP Full-Paket (indikativ)



ROI-BLICK FÜR DIE GESCHÄFTSLEITUNG

Unveränderte offene Funde entsprechen etwa **€972.500** indikativem offenem Rest-Risiko (Prioritätsleiter-Katalogeuro zur Priorisierung — keine Prognose eines realen Breach-Schadens). Das Schließen der drei höchsten Pfade in dieser Woche (SSO-MFA, geleakte Zugangsdaten, öffentliche Nicht-Produktion) würde das auf etwa **€175.000** senken — rund **€797.500** vermeidbare Exposition. Gegen ein illustratives SHELL-AFFECT-**CASP Full**-Paket von **€19.900** ergibt sich für dieses Muster eine Größenordnung von etwa **40×** Rest-Risiko-Kontrast (öffentlich: Lite ab €7.500 · Full €19.900 · Re-Investigation €4.500).

Offenes Rest-Risiko je Fund

Offener Fund	Prio	Risiko	Indikative Kosten
Öffentlicher SSO-/Anmelde-Host	P0	4	€375.000
Mitarbeiteridentitäten / Postfach-Korpus	P1	2	€85.000
Gebundene geleakte Zugangsdaten (3 Paare)	P0	4	€375.000
Öffentlicher Nicht-Prod-/Staging-Cluster	P1	3	€85.000
E-Mail-Auth. unter Reject	P2	2	€15.000
Öffentliche Datei mit Pen-Test-Titel	P2	1	€7.500
Vendor- / verwandte Domain-Oberfläche	P2	2	€15.000
Technologie-Fingerprint (Hinweis)	P2	2	€15.000
Summe offenes Rest-Risiko			€972.500

Pfadbezogene Exposition (nicht additiv)

Pfad (Relativrang)	Stufe	Kostentreiber	Pfadkosten
#1 Öffentl. Login	Kritisch	SSO-Edge + Mitarbeiteridentitäten (P0 × Risiko 4)	€125.000
#2 Credential-Leaks	Hoch	3 gebundene E-Mail/Passwort-Paare (P0 × Risiko 4)	€125.000
#3 Staging-Systeme	Hoch	Öffentlicher Nicht-Prod-/Proxy-Cluster (P1)	€85.000
#4 E-Mail-Spoofing	Mittel	SPF soft-fail + DMARC quarantine (P2)	€15.000
#5 Öffentl. Dateien	Niedrig	Öffentliche Datei mit Pen-Test-Titel (P2 × Risiko 1)	€7.500
#6 Executive-Phishing	Hoch	Führung + Postfach (teilt Login-Oberfläche)	€125.000
#7 Finanzbetrug	Hoch	BEC-/Zahlungsbetrug-Pretext (P1)	€85.000
#8 Vendor-Trust	Hoch	Vendor-Imitationsfläche (P1)	€85.000
#9 Tech-Fingerprint	Hoch	Tech-Fingerprint / KEV-Hinweis (P2)	€15.000

Pfadkosten werden nicht zum Portfolio-Gesamtwert addiert — überlappende Belege würden doppelt zählen. Das Portfolio-Rest-Risiko ist die Summe der einzelnen offenen Funde oben.

Wie diese Zahlen berechnet werden

Die Beträge sind **indikative Rest-Risikokosten** zur Priorisierung und ROI-Diskussion — derselbe Monetarisierungsansatz wie in der CASP-Plattform (offene Restexposition gegenüber Einsparungen, sobald Funde geschlossen sind). Sie sind **keine** Schadensprognose, kein Versicherungsangebot und keine Schätzung regulatorischer Bußgelder.

Berechnung. Jeder offene Fund erhält eine Prioritätsbandbreite und ein Risikolevel (1–4). Basisbänder folgen der CASP-Prioritätsleiter: P0 = €250.000 · P1 = €85.000 · P2 = €15.000. Risiko skaliert die Basis: Risiko 4 ×1,5 · Risiko 2–3 ×1,0 · Risiko 1 ×0,5 (z. B. P0 × Risiko 4 = €375.000). **Portfolio-Rest-Risiko** = Summe der einzelnen offenen Funde (als behoben oder nicht zutreffend markierte Funde zählen als €0). **Pfadkosten** = nicht-additive Aggregation (typisch das Maximum der stützenden offenen Funde, damit überlappende Pfade im Portfolio-Gesamtwert nicht doppelt zählen). „Nach Top-3-Fixes“ unterstellt, dass starke Mehrfaktor-Authentifizierung die Login-Edge-Kosten um ca. 90 % senkt und die Funde zu geleakten Zugangsdaten sowie öffentlicher Nicht-Produktion geschlossen sind.

Quellen und Kalibrierung (nicht willkürlich). Zwei Anker setzen die Größenordnung: (1) **IBM Cost of a Data Breach Report** (IBM Security / Ponemon-Institute-Methodik) — die verbreitete Branchenstudie zu den **durchschnittlichen organisationsbezogenen Kosten eines eingetretenen Data Breach** (in aktuellen Ausgaben im mehrstelligen Millionenbereich EUR/USD; globale und regionale Mittelwerte schwanken je Jahr). CASP übernimmt diesen Mittelwert **nicht**

als Rest-Risiko; er dient als externer Deckel-/Kontext, damit Prioritätsbänder board-tauglich bleiben, ohne jeden offenen Fund als Voll-Breach darzustellen. (2) Der CASP-Katalog indikativer Kosten — rund 95 Bedrohungstypen (Company Information, Infrastructure, Leaks) mit Min-/Avg-/Max-Kosten, Stand Januar 2026. Die transparente betriebliche Leiter **P0 €250.000 · P1 €85.000 · P2 €15.000** ist eine bewusste Vereinfachung dieser Katalogspannen, **deutlich unter** typischen IBM-Einzel-Breach-Mittelwerten skaliert, weil CASP **offene Expositionen** priorisiert und keinen gemessenen Breach-Vorfall abbildet. Gleicher Ansatz wie in Produktions-Assessments und der Verfolgung offener Restkosten. Die Zahlen bleiben **indikativ** zur Priorisierung — keine Schadensprognose, kein Versicherungsangebot und kein aktuarielles Modell. Das illustrative CASP-Full-Paket (€19.900) dient nur dem ROI-Kontrast in diesem Muster, nicht als verbindliches Angebot. Öffentliche Einstiege: CASP Lite ab €7.500; CASP Full €19.900; Re-Investigation €4.500 pro Durchlauf.

1.2 Methode und Leseführung

Die Erhebung nutzte ausschließlich öffentliche Quellen — kein Login, kein authentifiziertes Testing, kein Scannen der Origins. Feststellungen sind nach externer Sichtbarkeit, priorisiertem Angriffspfad und empfohlener Maßnahme gruppiert. Belege sind einer einfachen sechsstufigen Angriffskette (Abbildung A) zugeordnet, damit Verantwortliche sehen, wo öffentliche Daten Aufklärung, Zustellung oder Ausnutzung stützen.

1.3 Referenz Angriffskette

Die Stufen 1–4 sind dort am stärksten, wo passives OSINT greift. Stufen 5–6 brauchen oft Bestätigung durch Ihr Team (echte MFA-Lage, Zahlungskontrollen, ob Staging Produktionsdaten hält).

Abbildung A — Stufen der Angriffskette. Der obere Balken zeigt, wie viel CASP extern beobachten kann.

1.4 Scorecard

Thema	Ergebnis	Implikation
Offenes Rest-Risiko	€972.500 indikativ	Katalogkosten, wenn offene Funde unverändert bleiben
Wenn Ränge #1–#3 geschlossen	€175.000 Rest	≈ €797.500 diese Woche vermeidbar
Pfad Rang #1	Öffentliches Login + Identitäten (Kritisch, 84)	Pfadkosten €375.000 · Phishing / Credential-Stuffing am SSO
Pfad Rang #2	Offengelegte Zugangsdaten in Leak-Daten (Hoch, 71)	Pfadkosten €375.000 · Wiederverwendung am Login
Pfad Rang #3	Öffentliches Staging / Proxy (Hoch, 74)	Pfadkosten €85.000 · schwächerer Edge; wachsender Cluster

Thema	Ergebnis	Implikation
Pfad Rang #4	E-Mail-Auth. unter Reject (Mittel, 60)	Pfadkosten €15.000 · SPF soft-fail; DMARC quarantine
Hoher Score, niedriger Rang	Tech-Fingerprint (Hoch, 78) Rang #9	Stack-/KEV-Boost ≠ bestätigte Notlage bei selbst gehosteten Systemen
Zugangsdaten-Abdeckung	Abgeschlossen — 3 gebundene Paare (Muster)	Passwort-Resets erzwingen; Sitzungen beenden; Wiederverwendung prüfen
Offene Aktionen	20 (4 dringend, 16 wichtig)	Diese Woche zuweisbar
Tempo	+20 Hosts; 6 hochsignifikante Punkte weiterhin offen; +9 Nicht-Produktion	Staging-Wachstum bei ungelösten Angriffsflächen über mehrere Scans
Öffentliche Hosts	Etwa 60+	Vollliste im technischen Datensatz; Stichprobe in §3

1.5 Risikobild

Abbildung 1 — Pfade nach CASP-Score (Farbe = Schwere). Relativer Rang in §4 kann von der Score-Reihenfolge abweichen (siehe Tech #9).

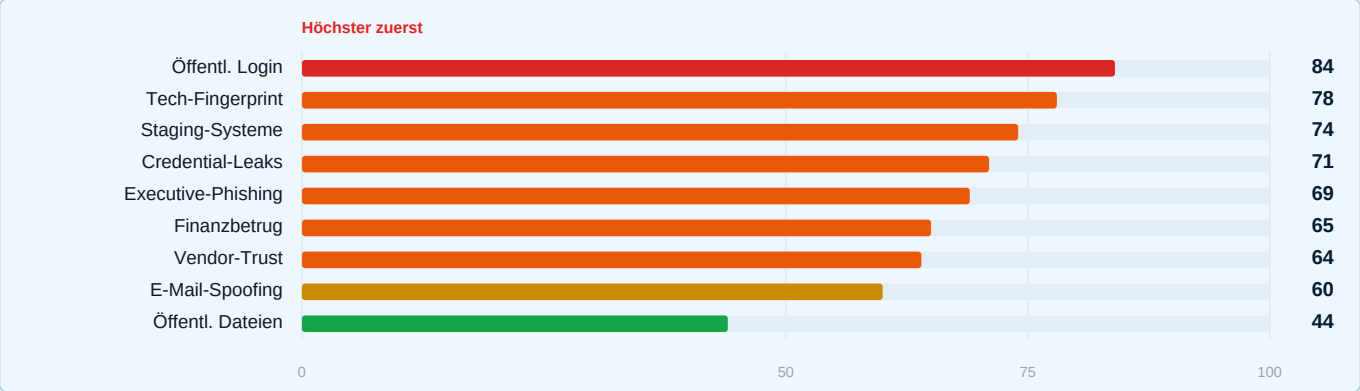
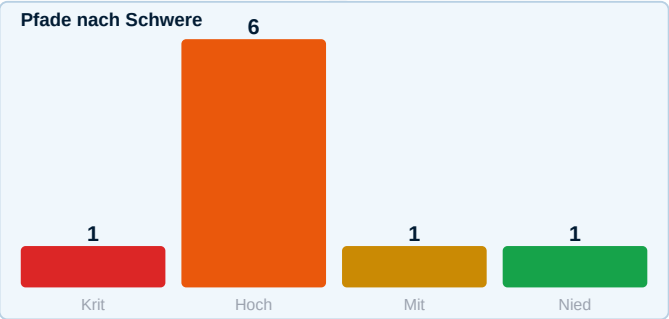
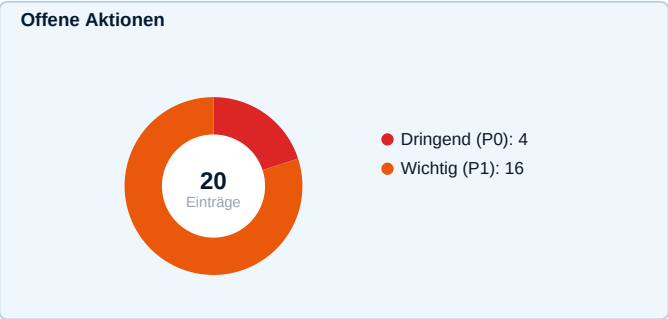


Abbildung 2 — Pfadschwere (links) und offene Aktionen (rechts).

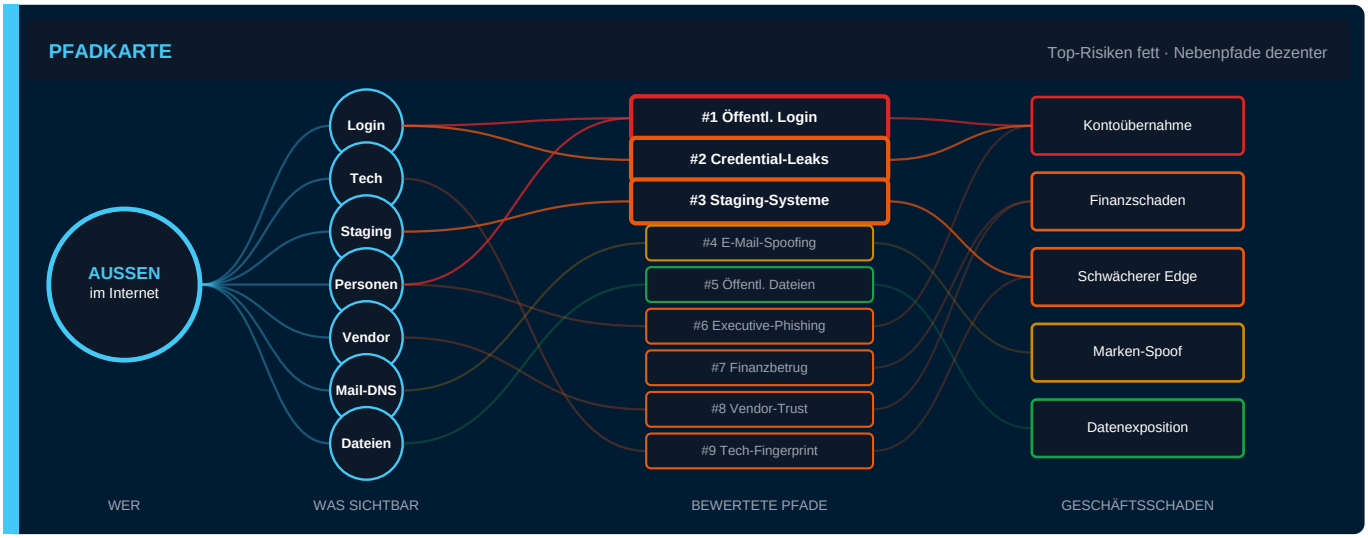




1.6 Pfadkarte

Von links nach rechts: externer Beobachter → sichtbare Assets → Pfade nach CASP-Priorität → Auswirkung. Die drei höchsten Ränge sind hervorgehoben (nicht immer der höchste Roh-Score).

Abbildung 3 — Pfadkarte. Hervorgehobene Pfade (#1–#3 nach Priorität) sind das Briefing-Set.



1.7 Prioritäre Maßnahmen

Prio	Maßnahme	Verantwortlich	Warum jetzt
Dringend	Phishing-resistente MFA am öffentlichen SSO; reines Passwort-Login reduzieren	Identity / IT	#1 · €375.000 Pfadkosten
Dringend	Erzwungenes Zurücksetzen und Beenden aktiver Sitzungen für betroffene Konten	SecOps / Identity	#2 · €375.000; Paare am SSO
Wichtig	Öffentliches Staging/Proxy entfernen oder schützen	Platform	#3 · €85.000; Cluster wächst
Wichtig	DMARC Richtung reject; SPF/DKIM härten	Messaging	#4 · €15.000; SPF soft-fail
Wichtig	Öffentliche Datei mit Pen-Test-Titel prüfen	Security	#5 · €7.500; Marketing vs. echt
Wichtig	SaaS-Hersteller-KEV/Hinweise überwachen (z. B. Kollaborations-Cloud)	AppSec	KEV-Familie; kein Versionsnachweis — nur Herstellerhinweis

Wenn diese Woche nur zwei Punkte landen: öffentliches SSO härten (#1) und geleakte Zugangsdaten zurücksetzen (#2). Danach Nicht-Produktion schließen (#3) und E-Mail-Auth. Richtung reject heben (#4). Zusammen senken die Ränge #1–#3 das indikative Rest-Risiko um etwa €797.500. Rest-Risiko hängt weiterhin von MFA-Lage, beabsichtigten Demos und Vier-Augen-Prinzip bei Zahlungen ab.

2. Geltungsbereich und Grenzen

Im Geltungsbereich: die öffentlich sichtbare Oberfläche von **northline-ready.example** — Hostnamen, DNS, Personen und E-Mails in offenen Quellen, öffentliche Dateien und extern erkennbare Drittanbieter.

Außerhalb des Geltungsbereichs: aktives Scannen, authentifiziertes Testen, Marken-Takedown, Malware-Analyse, interne Netze, Rechtsberatung.

Grenzen dieses Musterlaufs:

- Zugangsdaten-Abdeckung gegen öffentliche Leak-Datenbanken abgeschlossen — nur domänengebundene, geprüfte Paare werden ausgewiesen.
- Exakte Software-Versionen sind extern selten sichtbar; Cloud-Herstellerhinweise sind meist Sache des Vendors.
- Öffentliche Funding- oder Größenangaben gelten nicht als geprüfte Fakten.
- Die Oberfläche ist ein Snapshot und ändert sich.

2.1 Außenansicht und innere Einschätzung

Sicht	Quelle	Beantwortet
Außen (dieser Bericht)	CASP-Passive-Erhebung	Was ist sichtbar? Welche Pfade sind priorisiert?
Innen (Ihr Team)	IT, Security, Operations	Echt, beabsichtigt oder bereits behoben?
Lücke	Wo beides auseinanderfällt	Entfernen, einschränken, härten oder mit Note akzeptieren?

Im Ticketsystem / Remediation-Log erfassen Sie eine innere Disposition je Item (resolved, false positive, disclosed — mit kurzer Note). Dieses PDF friert einen Muster-Snapshot ein.

3. Externes Inventar

Repräsentative Stichproben für Entscheidungen. Vollständige Host- und Adresslisten liegen im technischen Datensatz.

3.1 Themen

Thema	Umfang	Stufen	Implikation
Öffentliche Login-/Account-Hosts	SSO + Account-Flächen	1 · 4 · 6	Modulübergreifend: Mitarbeiter-E-Mails + erreichbares SSO
Geleakte Zugangsdaten (Leak-Datenbanken)	3 gebundene Paare (Muster)	1 · 4 · 6	Wiederverwendung am SSO; erzwungenes Zurücksetzen + Sitzungsprüfung
Nicht-Produktion + Proxy-Edges	Dutzend+ Dev/Staging/Proxy	1 · 4 · 5	Cluster-Wachstum; Layout-Hinweis; schwächere Auth
Personen und Postfächer	Führung + ~10 Mitarbeiterbeispiele	1 · 3 · 6	Zustelllisten; BEC / Spear-Phishing-Vorwand
Drittanbieter-Dienste	CDN, Mail, Pay, Kollaboration	1 · 2 · 3	Vendor-Köder; KEV-Familien-Monitoring
Öffentliche Dateien	≥1 Datei mit Pen-Test-Titel	1 · 6	Titel signalisiert Sensibilität; Sample/Marketing klären

3.2 Hostnamen-Stichprobe

Hostname	Klasse	Stufen	Implikation
sso.northline-ready.example	Login	1→4	Primäres Authentisierungsziel
account.northline-ready.example	Account	1→4	Sekundäres Login / Lebenszyklus
academy.northline-ready.example	Produkt	1	Produktfläche für Recon
airflow.data-dev.northline-ready.example	Staging	1→4	Datenplattform; Nicht-Produktion-Edge
analytics-dev.northline-ready.example	Staging	1→4	Nicht-Produktion Analytics
app-test.northline-ready.example	Staging	1→4	Test-Namen signalisieren niedrigere Absicherungen
dbt.data-dev.northline-ready.example	Staging	1→4	Daten-Werkzeuge am Nicht-Produktion-Edge
proxy.academy.northline-ready.example	Proxy / Edge	1→4	Proxy-Namen erweitern Angriffsflächenkarte

Hostname	Klasse	Stufen	Implikation
proxy.ent-staging.northline-ready.example	Proxy / Staging	1→4	Enterprise Nicht-Produktion-Proxy
k8s.flock-ng-dev.northline-ready.example	k8s / Staging	1	Cluster-Namen leaken Topologie
northline-solutions.example	Verwandte Domain	1→3	Verwandte Marken-Domain (Supply / Recon)
…	…	…	≈50 weitere Hosts im vollständigen Datensatz

3.3 Personen- und E-Mail-Stichprobe

Identität	Kontext	Stufen	Implikation
A. Varga	CEO (öffentlich)	1→3→6	Autoritätsvorwand (BEC)
a.varga@northline-ready.example	Executive-Postfach	1→3	Spear-Phish-Zustelladresse
T. Fernandez	Revenue Leadership (öffentl.)	1→3→6	Finance-/Sales-Pretext
s.chen@northline-ready.example	Mitarbeiter-Sample	1→3→4	Phish-Liste; SSO-Credential-Stuffing-Kandidat
m.okonkwo@…	Mitarbeiter-Sample	1→3→4	Phish-Liste; SSO-Credential-Stuffing-Kandidat
…	Vollpack (~10 Samples)	…	Weitere Adressen erweitern die Zustellmenge

3.4 Exposition von Zugangsdaten (Leak-Datenbanken)

Subjekt (maskiert)	Typ	Bindung	Implikation
s.chen@northline-ready.example	E-Mail + Passwort-Paar	Stark (Domain-Match)	Replay an sso / account Hosts
m.okonkwo@northline-ready.example	E-Mail + Passwort-Paar	Stark (Domain-Match)	Replay an sso / account Hosts
ops-bot@northline-ready.example	E-Mail + Passwort-Paar	Stark (Domain-Match)	Service-Postfach; hohes Risiko bei Wiederverwendung
Klartext-Geheimnisse nicht gedruckt	Policy	—	Volle Digests nur im technischen Datensatz / Ticketsystem

3.5 Externe Dienste

Dienst	Rolle	Stufen	Implikation / Kontrolle
Cloudflare	DNS / Edge	1	Edge-Posture; Origin separat härten
Google Workspace	Unternehmens-E-Mail	3→4	Zustellkanal und Post-Phish-Ziel
OnDMARC-Klasse Mail-Stack	SPF / DMARC-Tooling	2→3	SPF soft-fail; DMARC quarantine heute
Stripe / Recurly	Zahlungen (JS)	1→2	Payment-Themen in Ködern; Scripts inventarisieren
Atlassian Cloud	Kollaborations-SaaS	1→2	KEV-Familie — Vendor monitoren (keine Version gesehen)
HubSpot	Marketing	1→2	Öffentliche Scripts erweitern Fingerprint; ungenutzte entfernen

4. Angriffspfade

Scores vergleichen relative Pfadstärke aus passiven Belegen. Sie sind **keine** Breach-Wahrscheinlichkeiten. **Rang folgt dem CASP-Relativrang** (Priorisierung für Operatoren), nicht dem Roh-Score allein. Ein hoher Score kann niedriger ranken, wenn Boosts gedeckelt sind (z. B. SaaS-KEV ohne bestätigte selbst gehostet-Version).

#	Pfad	Score	Schwere	Stufen	Auswirkung
1	Öffentliches Login und Mitarbeiteridentitäten	84	Kritisch	1→3→4→6	Kontoübernahme
2	Offengelegte Zugangsdaten in öffentlichen Leak-Daten	71	Hoch	1→4→6	Kontoübernahme
3	Öffentliche Staging- und Testsysteme	74	Hoch	1→4→5	Schwächerer Edge-Zugang
4	Risiko der Domain-E-Mail-Fälschung	60	Mittel	2→3	Marken-Spoofing
5	Öffentliche Datei mit Titel wie interner Pen-Test-Bericht	44	Niedrig	1→6	Datenexposition
6	Gezieltes Phishing gegen Führungskräfte	69	Hoch	1→3→4→6	Kontoübernahme
7	Finanzbezogener Zahlungsbetrug (BEC)	65	Hoch	1→3→6	Finanzieller Schaden
8	Imitation vertrauenswürdiger Lieferanten	64	Hoch	1→3→6	Finanzieller Schaden
9	Sichtbarer Technologie-Fingerprint	78	Hoch	1→2	Targeting-Effizienz

Hinweis: Tech-Fingerprint scored **78 (Hoch)**, rangt aber **#9** — Stack-/KEV-Aufschlag mit Stufenobergrenze. Exposition von Zugangsdaten rangt **#2**, wenn die Abdeckung der Leak-Datenbanken gelingt und Paare an die Domain binden. E-E-Mail-Auth. scored **60 (Mittel)**, rangt aber **#4** als praktischer Zustellverstärker.

Details unten: Ränge #1–#3 (Login, geleakte Zugangsdaten, Staging), plus Mail (#4) als Zustellverstärker. Tech-Fingerprint (#9) hat hohen Score / niedrigeren Rang — siehe Hinweis zur Tabelle. Weitere Pfade in §4.1.

PATH-01 · Öffentliches Login und Mitarbeiteridentitäten

Kritisch · 84

Feststellung

Öffentlicher Anmelde-Host **sso.northline-ready.example** ist erreichbar. Etwa zehn Mitarbeiter- und Executive-Identitäten erscheinen in offenen Quellen. Modulübergreifend: E-Mails + SSO stützen gezieltes Phishing und Credential-Stuffing gegen eine echte Authentisierungsgrenze. Mit abgeschlossener Leak-Abdeckung (PATH-02) ist Credential-Stuffing nicht mehr theoretisch. Beispiel-Adressen: 203.0.113.10 / 203.0.113.11.

Belege

sso.northline-ready.example; account.northline-ready.example; 203.0.113.10 / 203.0.113.11; Postfächer a.varga@northline-ready.example, s.chen@northline-ready.example (weitere Beispiele im Paket). Score-Hinweis: strukturell 72 · Bestätigung 8 · Sektor-Aufschlag.

Angriffskette: 1 → 3 → 4 → 6 (Kontozugriff)

Nutzung der Belege entlang der Kette

Stufe	Genutzte Belege	Wirkung
1 · Aufklärung	sso.northline-ready.example; Mitarbeiternamen	Wer arbeitet hier und wo wird authentisiert

Stufe	Genutzte Belege	Wirkung
3 · Zustellung	a.varga@…, s.chen@…	Phishing- oder Passwort-Reset-Köder an reale Personen
4 · Ausnutzung	Öffentliches SSO / Passwort-Fläche	Gestohlene, geleakte oder geratene Zugangsdaten; MFA-Ermüdung
6 · Ziel	Session / Postfach / App-Zugang	Mail lesen, Zahlungen, seitlicher Bewegung mit vertrauenswürdiger Identität

Vorbehalt

Niedrigere Priorität, wenn der Host nur Marketing ist oder Anmeldung phishing-resistente MFA ohne Passwort-Rückfalloption verlangt.

Empfohlene Maßnahmen

- Phishing-resistente MFA an SSO, VPN und Mail erzwingen
- veraltete Authentisierungsmethoden wo möglich deaktivieren
- Admin-Portale vom öffentlichen Internet nehmen oder hinter Zero Trust
- Unnötige öffentliche Rollen-Postfächer reduzieren

PATH-02 · Offengelegte Zugangsdaten in öffentlichen Leak-Daten

Hoch · 71

Feststellung

Abdeckung der Leak-Datenbanken für diesen Musterlauf abgeschlossen. CASP hat **3 E-Mail/Passwort-Paare** an northline-ready.example gebunden (Störsignale gefiltert; ungebundene/Marketing-Treffer zurückgehalten). Zusammen mit öffentlichem SSO stützen diese Geheimnisse Credential-Stuffing und Kontoübernahme ohne Phishing. Klartext-Geheimnisse stehen nicht in diesem PDF — Digests liegen im technischen Datensatz / Ticketsystem.

Belege

Subjekte (im Bericht maskiert): s.chen@northline-ready.example, m.okonkwo@northline-ready.example, ops-bot@northline-ready.example; Wiederverwendung-Fläche sso.northline-ready.example / account.northline-ready.example. Abdeckungsstatus: abgeschlossen; Veröffentlichung freigegeben; 3 gebundene Paare.

Angriffskette: 1 → 4 → 6 (Wiederverwendung → Zugang)

Nutzung der Belege entlang der Kette

Stufe	Genutzte Belege	Wirkung
1 · Aufklärung	Leak-Datenbanken + Domain-Bindung	Welche Org-Adressen mit Geheimnisse erscheinen
4 · Ausnutzung	sso.northline-ready.example / Account-Hosts	Geleakte Passwörter oder Credential-Stuffing-Listen
5 · Fuß fassen	authentisierte Session	Session-Wiederverwendung bei schwacher/fehlender MFA
6 · Ziel	Postfach / App / API-Zugang	Datendiebstahl, Betrug oder seitliche Bewegung

Vorbehalt

Niedrigere Priorität, wenn Passwörter bereits rotiert, Konten deaktiviert oder Paare nicht an Live-Konten binden.

Empfohlene Maßnahmen

- Erzwungenes Passwort-Zurücksetzen und aktive Sessions für betroffene Konten widerrufen
- Passwort-Wiederverwendung an VPN, SSO, Mail und Admin-Tools prüfen; MFA überall
- Service-Account-Geheimnisse rotieren; Zugangsdaten in Geheimnisspeicher verlagern
- Verdächtige Logins im Expositionsfenster jagen

PATH-03 · Öffentliche Staging- und Testsysteme

Hoch · 74

Feststellung

Mehrere Nicht-Produktion- und Proxy-Hostnamen resolven öffentlich unter northline-ready.example (data-dev, analytics-dev, app-test, dbt, k8s-*-dev, proxy.academy, proxy.enterprise-staging). Namen verraten Layout und sitzen oft hinter schwächeren Absicherungen als Produktion. Tempo: Nicht-Produktion-Cluster wächst, während frühere hochsignifikante-Hosts offen bleiben.

Belege

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 (Vollliste im Datensatz).

Angriffskette: 1 → 4 → 5 (möglicher Fuß fassen)

Nutzung der Belege entlang der Kette

Stufe	Genutzte Belege	Wirkung
1 · Aufklärung	*-dev / Staging / Proxy / k8s-Namen	Mappt Umgebungsform aus öffentlichem DNS
4 · Ausnutzung	Öffentliche Nicht-Produktion-Edges	Schwächere Auth, vergessene Testkonten
5 · Fuß fassen	Nicht-Produktion als Brückenkopf	Risiko, wenn Staging Produktion vertraut (innen bestätigen)
6 · Ziel	Daten oder Config auf Staging	Kundendaten oder Geheimnisse in Nicht-Produktion

Vorbehalt

Niedrigere Priorität, wenn Staging eine beabsichtigte öffentliche Demo ohne Pfad zu Internem/Kundendaten ist.

Empfohlene Maßnahmen

- Öffentliches DNS für Nicht-Produktion und Proxy entfernen oder starke Auth verlangen
- Sicherstellen, dass Staging keine Produktionssecrets/Kundendaten hält
- Staging-Zugangsdaten von Produktion trennen
- Intentionale öffentliche Demos als genehmigte Exceptions dokumentieren

PATH-04 · Risiko der Domain-E-Mail-Fälschung

Mittel · 60

Feststellung

E-E-Mail-Auth.entisierung für northline-ready.example liegt unter einer Hard-Fail-Policy. Beobachtete Posture (öffentliches DNS): **SPF soft-fail (~all)** und **DMARC quarantine bei 100%** — nicht reject. Das erleichtert weiterhin Nachrichten, die von Ihrer Domain zu stammen scheinen, und verstärkt PATH-01 / BEC / Vendor-Fraud.

Belege

Öffentliche DNS-Mail-Matrix: SPF soft-fail; DMARC p=quarantine pct=100; DKIM-Selektoren in diesem Musterpack nicht vollständig gemappt.

Angriffskette: 2 → 3 (Verstärker für PATH-01 / BEC)

Nutzung der Belege entlang der Kette

Stufe	Genutzte Belege	Wirkung
2 · Vorbereitung	SPF soft-fail · DMARC quarantine	Prüft, ob die Domain günstig spoofbar ist
3 · Zustellung	From: wirkt wie Ihre Domain	Höheres Vertrauen für BEC und Marken-Phish

Stufe	Genutzte Belege	Wirkung
4 · Ausnutzung	Nutzer handelt auf gefälschte interne Mail	Zugangsdaten-Harvest oder Zahlungsanweisung
6 · Ziel	Betrug oder Postfachzugriff	Geldfluss oder Identitätsmissbrauch

Vorbehalt

Niedrigere Priorität, wenn DMARC reject ist, SPF auf -all endet, DKIM alle legitimen Sender abdeckt und Reports überwacht werden.

Empfohlene Maßnahmen

- Jeden legitimen Outbound-Sender inventarisieren
- DKIM auf allen Sendeströmen aktivieren
- DMARC von quarantine auf reject heben
- DMARC-Aggregat-Reports bis zur Stabilität prüfen

4.1 Sekundäre Pfade

#	Pfad	Score	Stufen	Kurz	Verantwortlich
5	Pen-Test-titelte öffentl. Datei	44	1→6	Titel suggeriert interne Feststellungen — Marketing-Muster vs. echte Exposition klären	Security
6	Executive-Phishing	69	1→3→4→6	CEO + Leadership-Postfächer → gezielte Zustellung → Login-Missbrauch	Identity
7	Finance-BEC	65	1→3→6	Öffentlicher Funding-/Finance-Kontext → gefälschte Zahlungsanweisung	Finance
8	Vendor-Imitation	64	1→3→6	Sichtbare Provider + verwandte Domain → gefälschte Vendor-Änderungen	Procurement
9	Tech-Fingerprint	78	1→2	Hoher Score, niedriger Rang — SaaS-KEV nur Herstellerhinweis ohne Versionsnachweis	AppSec

Pfade #6–#8 verstärken vor allem **PATH-01 / PATH-02**, wenn öffentliches Login, geleakte Geheimnisse und E-E-Mail-Auth. unter Reject bereits existieren. Pfad #5 ist niedrig im Score, aber leicht zu verifizieren (URL noch öffentlich?).

5. Externe Technologie-Exposition

Extern sichtbare Drittanbieter — kein internes SBOM. Marketing-Namen sind keine Partner. Wettbewerber allein rechtfertigen keinen Supply-Chain-Pfad. KEV-Treffer ohne beobachtete Versionen sind **Produktfamilien-Risiko**, kein Beweis für einen verwundbaren Build.

Priorität	Signal	Komponente	Maßnahme
Wichtig	KEV-Klasse (Muster CVE-2023-22527)	Kollaborationoration SaaS (Cloud)	Herstellerhinweis monitoren; Mandanten-Auswirkung klären
Wichtig	KEV-Klasse (Muster CVE-2021-26086)	Kollaborationoration SaaS (Cloud)	Herstellerüberwachung — kein selbst gehostet-Notfall
Wichtig	5 KEV-Treffer · keine Versionen beobachtet	Atlassian-Klasse Cloud-Produkte	Ehrlichkeit: SaaS → nur Herstellerhinweis, außer selbst gehostet belegt
Wichtig	Öffentliche Payment-/Marketing-Scripts	Stripe / Recurly / HubSpot	Scripts inventarisieren; ungenutzte entfernen

6. Maßnahmen-Tracker

Dringend: ~7 Tage. Wichtig: ~14 Tage. A-01 deckt Rang #1 (Login). A-02 deckt Rang #2 (geleakte Zugangsdaten). A-03 deckt Rang #3 (Nicht-Produktion). A-04 deckt Rang #4 (Mail).

ID	Prio	Maßnahme	Verantwortlich	Fällig	Erledigt wenn
A-01	Dringend	Öffentliches Login härten (sso.northline-ready.example)	Identity	7d	Phishing-resistente MFA; Legacy-Auth aus
A-02	Dringend	3 gebundene Leak-Konten zurücksetzen/rotieren	SecOps	7d	Resets erledigt; Sitzungen beenden; Wiederverwendung-Hunt sauber
A-03	Wichtig	Öffentliches Staging / Proxy entfernen oder schützen	Platform	14d	Kein öffentliches Nicht-Produktion ohne starke Auth
A-04	Wichtig	E-E-Mail-Auth. Richtung reject (SPF/DKIM/DMARC)	Messaging	14d	DMARC reject oder dokumentierte Ausnahme
A-05	Wichtig	Pen-Test-titelte öffentliche Datei prüfen	Security	14d	URL privat/weg oder als öffentliches Sample akzeptiert
A-06	Wichtig	Vendor über einen zweiten Kanal + Partner-MFA	Procurement	14d	Prozess live; MFA enforced

7. Änderung seit vorheriger Erhebung

Gegenüber einem früheren Musterfenster: **+20 Hosts**, darunter ein **+9 Nicht-Produktion-/Staging-/Proxy-Cluster** (erhöhtes Zeitfenster). **6 hochsignifikante-Flächen bleiben über Collections offen** (Aging). Höchster Restdruck: öffentliches Login (Rang #1) und Nicht-Produktion-Wachstum (Rang #3). Score-Kalibrierung hat mehrere Pfade von früheren überhöhten Decken gesenkt — die Rangordnung ist stabiler als der Roh-Score allein.

8. Empfohlene nächste Schritte

Schritt	Wer	Maßnahme
1	Security-Leitung	Briefing der Führung nur aus §1 (~5 Minuten)
2	Identity / Platform	A-01 und A-02 annehmen oder hinterfragen (Anhang A)
3	Item-Verantwortliche	Disposition im Ticketsystem / Remediation-Log setzen (Anhang B)
4	Security-Leitung	Re-Scan; Anhang-A-Abschlusskriterien bestätigen

30- / 90-TAGE-ERGEBNISSE

30 Tage: phishing-resistentes öffentliches Login, Leak-Konten resettet, kein unnötiges öffentliches Staging, E-E-Mail-Auth. Richtung reject. 90 Tage: aging Items nach Re-Scan geklärt, Vendor-Prozess dokumentiert, Re-Scan zeigt Paare weg oder rotiert. Operator-Detail: Anhänge A–C.

Anhang A — Abschluss-Checklisten

Druckbare Verifikation für dringende und wichtige Arbeitsstränge. Offline abhaken falls nötig, dann die passende Disposition im Ticketsystem / Remediation-Log erfassen (Anhang B). Aktions-IDs entsprechen §6.

A.1 PATH-01 / A-01 — Öffentliches Login · Dringend

Primärpfad. Mit A-02 (geleakte Zugangsdaten) koppeln — gleiche SSO-Fläche.

	Maßnahme	Erledigt wenn	Nachweis / Re-Scan
☐	**Phishing-resistente MFA an sso.northline-ready.example (und verknüpftes VPN / Mail) erzwingen**	Passwort-only entfernt oder eng begrenzt	Öffentliches Login verlangt starke MFA; Legacy-Auth nicht angeboten
☐	**veraltete Authentisierungsmethoden am Identity-Edge deaktivieren**	Keine Basic-/Legacy-Protokolle aktiv	Identity-Konfiguration bestätigt Legacy deaktiviert
☐	**Admin-Portale einschränken (nicht welt-offen; ZTNA/Allowlist bevorzugt)**	Administrative Interfaces nicht öffentlich ohne starke Auth	Admin-Hostnamen abwesend oder access-controlled im Re-Scan
☐	**Unnötige öffentliche Rollen- und Funktionspostfächer reduzieren**	Nur begründete öffentliche Adressen bleiben	Staff- und Rollen-Mailbox-Inventar schrumpft im Re-Scan
☐	**Disposition für verwandte Funde im Ticketsystem / Remediation-Log erfassen**	Status Resolved oder False positive mit kurzer Note	Remediation-Log existiert; aging hochsignifikante Items klären

A.1b PATH-02 / A-02 — Geleakte Zugangsdaten · Dringend

Relativrang #2 bei erfolgreicher Abdeckung der Leak-Datenbanken. Keine Klartext-Passwörter in Tickets — Ticketsystem-Digests nutzen.

	Maßnahme	Erledigt wenn	Nachweis / Re-Scan
☐	**Erzwungenes Passwort-Zurücksetzen für gebundene Subjekte (s.chen@, m.okonkwo@, ops-bot@ auf northline-ready.example)**	Resets abgeschlossen; Nutzer ggf. über einen zweiten Kanal informiert	Identity-System zeigt Reset-Zeitstempel; Paare nicht mehr gültig
☐	**Aktive Sessions / Refresh-Tokens für betroffene Konten widerrufen**	Keine langlebigen Sessions aus dem Expositionsfenster	SSO/Session-Store-Purge bestätigt
☐	**Passwort-Wiederverwendung an VPN, Mail, Admin und Partner-Portalen jagen**	Wiederverwendung-Checks erledigt; MFA wo fehlend enforced	Stichprobe sauber; Ticketsystem-Note angehängt
☐	**Service-Account- oder Bot-Zugangsdaten aus demselben Corpus rotieren**	ops-bot (o. ä.) Geheimnisse im Geheimnisspeicher abgelegt und rotiert	Altes Secret deaktiviert; Monitoring ohne Wiederverwendung
☐	**Disposition für Zugangsdaten-Funde im Ticketsystem / Remediation-Log erfassen**	Status Resolved mit Note nach Re-Scan oder Bestätigung	Remediation-Log existiert; Aging klären

A.2 PATH-03 / A-03 — Staging, Proxy und Nicht-Produktion · Wichtig

Relativrang #3. Öffentliche Exposition entfernen statt nur dokumentieren. Inkl. proxy.* Edges.

	Maßnahme	Erledigt wenn	Nachweis / Re-Scan

☐	**Öffentliches DNS für Nicht-Produktion entfernen oder hinter starke Authentisierung legen**	Keine unauthentifizierten öffentlichen Dev-/Staging-/Test-Edges	Hostnamen resolven nicht mehr öffentlich oder verlangen SSO/VPN
☐	**Bestätigen, dass Staging keine Produktionssecrets oder echten Kundendaten hält**	Interne Bestätigung durch Platform-Verantwortlich dokumentiert	Keine sensiblen Dateien/Zugangsdaten an Staging-Hosts gebunden
☐	**Staging-Zugangsdaten von Produktion trennen**	Keine geteilten Prod-/Staging-Geheimnisse	Innen bestätigt; optional Zugangsdaten-Re-Check
☐	**Intentionale öffentliche Demos als genehmigte Exceptions dokumentieren**	Exception-Liste mit Verantwortlich und Review-Datum	Ticketsystem-Status Disclosed mit Exception-Note
☐	**Disposition für Staging-Funde im Ticketsystem / Remediation-Log erfassen**	Resolved, False positive oder Disclosed mit Note	Remediation-Log aktualisiert; Multi-Scan-Delta verbessert

A.3 PATH-04 / A-04 — E-E-Mail-Auth.entisierung · Wichtig

Relativrang #4 (Mittel 60). SPF soft-fail und DMARC quarantine heute — Richtung reject heben.

	Maßnahme	Erledigt wenn	Nachweis / Re-Scan
☐	**Jeden legitimen Outbound-Sending-Service inventarisieren**	Vollständige, geownedte Senderliste für SPF	SPF enthält nur bekannte legitime Sender
☐	**DKIM auf allen Sendeströmen aktivieren**	DKIM aligned für jeden legitimen Sender	Öffentliches DNS zeigt DKIM; Aggregat-Reports bleiben sauber
☐	**DMARC von Monitoring/Quarantine Richtung reject vorantreiben**	Policy reject oder zeitlich begrenzte dokumentierte Ausnahme	DMARC-Record und Policy per öffentlichem DNS verifiziert
☐	**DMARC-Aggregat-Reports mindestens zwei Wochen prüfen**	Keine ungeklärten Spoofing-Quellen offen	Innenprozess läuft; optional Re-Check der E-E-Mail-Auth.-Posture

A.4 Verbleibende wichtige Aktionen

	Maßnahme	Erledigt wenn	Nachweis / Re-Scan
☐	**A-02 — Leak-Konten-Resets abschließen (siehe A.1b)**	Alle gebundenen Paare resettet; Sitzungen beenden; Wiederverwendung-Hunt erledigt	Re-Scan oder Bestätigung; Ticketsystem-Status Resolved mit Note
☐	**A-05 — Pen-Test-titelte öffentliche Datei prüfen (und andere sensible Titel)**	URL privat/weg oder als beabsichtigtes öffentliches Sample mit Note akzeptiert	Datei reklassifiziert; Ticketsystem-Status Resolved, Disclosed oder False positive
☐	**A-06 — Vendor über einen zweiten Kanal und Partner-Portal-MFA**	Prozess live; MFA auf Partner-Portalen enforced	interne Bestätigung; Ticketsystem-Status Resolved mit Note
☐	**PATH-09 / Tech-Stack — Cloud vs. selbst gehostet klären; SaaS-KEV-Herstellerhinweise tracken**	Verantwortlich benannt; Herstellerhinweis-Abos aktiv; kein falscher selbst gehostet-Notfall	Wenn nur SaaS: Ticketsystem-Status Disclosed mit Herstellerüberwachung-Note

Anhang B — Disposition-Leitfaden (Ticketsystem / Remediation-Log-Vokabular)

Dieselben Statusworte in Tickets und im Ticketsystem / Remediation-Log nutzen, damit Außen (dieser Bericht) und Innen (Ihre Einschätzung) aligned bleiben. Ein Status pro Fund; immer kurze Note.

Status	Wann nutzen	Wer setzt	Was Re-Scan zeigen soll
Exposed	Noch öffentlich und actionable; Default nach Scan	System (Default) oder Operator beim Wiederöffnen	Item noch vorhanden / hochsignifikante
Disclosed	Echter Fund, aber akzeptiert/bekannt (z. B. beabsichtigte Demo) mit Absicherungen	Verantwortlich + Security-Leitung	Kann noch erscheinen; Aging mit Note akzeptiert
Resolved	Control angewendet; Risiko praktisch geschlossen	Verantwortlich; Security-Leitung verifiziert	Entfernt, gehärtet oder erfüllt Pfadkriterien nicht mehr
False positive	Kein reales Risiko für diese Org (falsche Bindung, nicht owned, nur Marketing)	Verantwortlich mit Beleg in Note	Soll Pfad-Scores nicht treiben; Re-Scan kann Roh-Host noch listen

REMEDIATION-LOG

Jeden Statuswechsel protokollieren (wer / wann / warum). Live-Status im Ticketsystem; dieses PDF ist ein eingefrorener Sample. Nicht resolved markieren ohne Re-Scan-Nachweis oder interne Bestätigung (Anhang A).

Anhang C — Bericht zum Ticketsystem / Remediation-Log mappen

Dieses PDF ist das Offline-Bewertungspaket. Das Ticketsystem ist die Live-Arbeitsumgebung. Beides zusammen nutzen.

Berichtsabschnitt	Ticketsystem-Ort	Operator-Aktion
§1 Zusammenfassung	Dashboard · Wichtige Funde · CASP-Ansicht	Führung briefen; Verantwortlich für A-01 / A-02 zuweisen
§3 Externes Inventar	Funde · Infrastructure / Leaks / Company	Nach Domain filtern; Items öffnen; Disposition setzen
§4 Angriffspfade + Anhang A	CASP-Ansicht / Pfaddetail · Funde	vorrangige Pfade bearbeiten; Anhang A abschließen; Remediation loggen
§6 Maßnahmen-Tracker (A-01…A-06)	Remediation / Risk-Performance	Open vs resolved tracken; Notes anhängen
Anhang B Dispositionen	Discovery-Status: exposed / disclosed / resolved / False positive	Status + Note; nie ohne Notiz lassen
§7 Tempo / Multi-Scan	Historische Scans / Aging-Items	Aging nach Fix + Re-Scan bestätigen

Übergaberegel. Was nicht im Ticketsystem mit Disposition und Note steht, ist nicht geschlossen — auch wenn ein Häkchen auf Papier gesetzt wurde.

Anhang D — Methode und Klassifikation

Erhebung. Nur öffentliche Quellen — kein Discovery-Traffic zu Ihren Origins. **Scoring.** Vergleichende Pfadstärke aus verknüpften Belegen und unabhängigen Quellen; schwache Pfade werden nicht zufällig Critical. **Qualität.** Störsignale zurückgehalten; Marketing gefiltert; Zugangsdaten-Paare nur bei Domain-Bindung publiziert (dieses Muster simuliert erfolgreiche Abdeckung der Leak-Datenbanken — kein Klartext im PDF); Cloud-SaaS-Treffer als Herstellerüberwachung, außer selbst gehostet-Beleg.

Angriffsketten-Modell. Stufen 1–6 sind ein vereinfachter operativer Rahmen für passives OSINT (kein vollständiges MITRE ATT&CK-Abdeckung;).

VERTRAULICH · MUSTER (ANONYMISIERT) · SHELL-AFFECT — VERTRAULICH — Nur für benannte Empfänger. Nicht ohne Genehmigung weiterleiten. Diese Datei ist ein anonymisiertes Muster (fiktive Organisation), keine Live-Kundenbewertung.

Dokumentenkontrolle. SA-CASP-SAMPLE-2026-08 · 2. August 2026 · Erzeugt 2026-08-02 · SHELL-AFFECT · CASP · Subjekt (Muster): Northline Cyber Readiness Ltd. (northline-ready.example) · Anonymisiertes Beispiel der offiziellen CASP-Struktur.

Ende des Berichts · SA-CASP-SAMPLE-2026-08 · SHELL-AFFECT · CASP · VERTRAULICH