DARKWATER ASSOCIATES

ILLUSTRATIVE CLIENT DELIVERABLE

External Exposure Baseline Report

A fictional example showing how DarkWater turns scattered external exposure signals into a prioritized business action plan.

PREPARED FOR
Northstar Legal Group (fictional organization)

ASSESSMENT WINDOW
August 10-17, 2026

SCOPE
1 organization, 3 domains, 3 approved identities

REPORT ID
DW-ILL-2026-018

ILLUSTRATIVE SAMPLE
No real client, credential, victim, or employer data.

DarkWater Associates LLC
darkwaterpi.com

EXECUTIVE SUMMARY

What leadership needs to know.

DarkWater identified one high-priority exposure signal and three additional issues that warrant owner validation. No active testing, account access, or credential validation was performed.

OVERALL EXPOSURE POSTURE	HIGH	MEDIUM	INFORMATIONAL
Elevated	**1**	**2**	**2**
Prompt validation recommended	Immediate owner review	Near-term action	Track or close

Top business concerns

1. An approved historical email identity appeared in a newly reviewed infostealer-style exposure record.
2. A recently registered look-alike domain could support impersonation or payment-redirection attempts.
3. A third-party document index exposed project references and author metadata tied to the fictional client.

First actions

1. Confirm whether the exposed identity remains active or supports password recovery.
2. Review sign-in activity and revoke sessions where the client determines it is appropriate.
3. Escalate the look-alike domain to legal, brand, or email-security owners.
4. Contact the affected third party through an approved vendor-risk process.

Analyst judgment

The findings do not prove current compromise. They identify plausible exposure paths that deserve validation because they connect approved identities, recent timing, and business-relevant context. DarkWater's value is the human review that separates meaningful signals from unrelated matches and then assigns a practical owner and next step.

EXPOSURE LANDSCAPE

Findings ranked for action.

Each item is scored using identity confidence, source confidence, recency, likely business impact, and the amount of owner validation still required.

F-01	Historical email identity in an infostealer-style exposure record	HIGH	Identity / SOC
F-02	Recently registered look-alike domain with potential impersonation value	MEDIUM	Legal / Brand
F-03	Third-party document index exposed project and author metadata	MEDIUM	Vendor Risk
F-04	Dormant public repository reference to a retired subdomain	INFO	IT / Dev
F-05	Stale certificate reference associated with a discontinued service	INFO	IT

Identity confidence

Strong match to an approved identity and company context.

Source confidence

Credible source category, but owner validation is still required.

Business impact

Could affect identity, vendor access, or impersonation risk.

Why the list is short

DarkWater does not pad reports with every passive observation. Duplicates, weak name matches, stale records, and findings without a credible business connection are filtered or placed in an appendix.

1

Credential and identity exposure

Approved domains, emails, aliases, and related identity references.

2

Ransomware and exposed documents

Claims, file indexes, filenames, metadata, and business references.

3

Impersonation and brand signals

Look-alike domains, profiles, and misleading identity use.

4

Third-party and infrastructure context

Vendor exposure and passive public signals requiring owner validation.

HIGH-PRIORITY FINDING

Historical email identity in an infostealer-style exposure record

HIGH

Potential connection to a personal or unmanaged browser context

IDENTITY CONFIDENCE	SOURCE CONFIDENCE	FIRST OBSERVED	RECOMMENDED OWNER
High	Moderate	Aug. 14, 2026	Identity / SOC

What was observed

A newly reviewed exposure record referenced an approved historical email address associated with the fictional organization. The record included a hostname pattern and browser-application reference consistent with information-stealer collection from a personal or unmanaged endpoint.

The illustrative evidence record is masked in this report. DarkWater did not test the credential, access an account, contact the user, or attempt to identify a device owner.

> **Plain-language meaning**
> An identity connected to the organization may have been collected from a compromised browser or device outside the managed corporate environment. The record may be stale, but it could still support password recovery, vendor access, or impersonation.

Why it matters

- Historical personal or secondary emails are often reused for account recovery.
- Vendor portals may not use the same controls as the corporate identity provider.
- Infostealer records can include more than passwords, such as browser context or session data.
- The signal could be used to craft believable fraud or password-reset attempts.

Recommended validation path

0-4 HOURS
Confirm identity ownership and whether the address remains active or supports recovery.

WITHIN 24 HOURS
Review sign-ins, revoke sessions, and reset credentials where the organization determines appropriate.

WITHIN 7 DAYS
Assess device context, vendor accounts, and follow-on impersonation or reset attempts.

Limitations: Exposure records are intelligence signals, not proof of current compromise. Availability, accuracy, and timeliness vary by source. Client-side validation is required.

WHAT THE SECURITY TEAM RECEIVES

Priority Intelligence Notification

A concise, decision-ready alert for a material finding. This example would be delivered to the named client contacts through the agreed secure channel.

DARKWATER NOTIFICATION

HIGH

Potential credential exposure associated with an approved company identity

NOTIFICATION ID	IDENTITY CONFIDENCE	SOURCE CONFIDENCE	STATUS
DW-PN-2026-014	High	Moderate	Client validation

What happened

DarkWater reviewed a new exposure record referencing an approved historical email identity and browser context that may be associated with an unmanaged endpoint.

Why the client should care

The identity may still support password recovery, vendor access, or believable impersonation. The record does not prove current compromise, but the combination of identity match, timing, and source context meets the agreed notification threshold.

Recommended actions

1. Confirm ownership and current use of the identity.
2. Review relevant corporate and vendor sign-in activity.
3. Reset credentials and revoke sessions where the client determines appropriate.
4. Monitor for password-reset attempts, suspicious vendor contact, or executive impersonation.

What DarkWater did

Reviewed the potential match, removed duplicates, assessed confidence and business relevance, masked sensitive evidence, and escalated to the named contact.

What DarkWater did not do

No account access, password testing, device access, employee contact, or active exploitation was performed.

Designed for fast handoff

The notification can be routed to a CISO, IT director, identity team, MSP, legal contact, or other named owner. The full report retains the evidence notes, limitations, and action tracking.

PRIORITIZED ACTION REGISTER

Turn findings into owned work.

Every finding is assigned a recommended owner, urgency, validation step, and completion status. The client remains responsible for operational decisions and remediation.

ID	ACTION	OWNER	PRIORITY	TARGET	STATUS
A-01	Confirm ownership and recovery use of the exposed historical email identity.	Identity	HIGH	4 hours	**Open**
A-02	Review recent sign-ins and revoke relevant sessions where appropriate.	SOC / IT	HIGH	24 hours	**Open**
A-03	Evaluate look-alike domain for blocking, monitoring, or legal action.	Legal / Brand	MEDIUM	3 days	**Assigned**
A-04	Notify vendor-risk owner of exposed project and author metadata.	Vendor Risk	MEDIUM	5 days	**Assigned**
A-05	Confirm retired subdomain is not referenced in active documentation or DNS.	IT / Dev	INFO	14 days	**Planned**
A-06	Document closure or risk acceptance for each finding.	Risk Owner	TRACK	30 days	**Planned**

Suggested monitoring scope

- Three company domains and approved variants
- Five approved company or executive identities
- Ransomware and extortion references
- Look-alike domains and impersonation indicators
- Material exposed-document and third-party signals

Recommended cadence

- Priority notification when threshold is met
- Monthly intelligence brief
- Quarterly trend review
- Annual re-baseline or after major organizational change

Value when nothing urgent appears

A monthly brief still documents reviewed source categories, new potential matches, eliminated false positives, action status, and a clear statement when no material change was observed.

HOW THE ASSESSMENT WORKS

Passive, authorized, and human-reviewed.

The standard baseline uses public and lawfully accessed intelligence sources. It is designed to identify exposure indicators and direct owner validation, not to prove that every signal represents a current incident.

1

Scope confirmation

Legal entity, domains, brands, identities, authorization, recipients, and time window are documented.

2

Collection and correlation

Approved identifiers are reviewed across selected exposure, ransomware, document, infrastructure, and impersonation sources.

3

Analyst validation

Duplicates, weak matches, stale references, and unrelated records are filtered or clearly qualified.

4

Business reporting

Findings are ranked by confidence, likely impact, urgency, owner, limitations, and recommended validation.

Standard boundaries

- No credential testing or account login
- No exploitation or penetration testing
- No personal-device agent installation
- No employee contact or social engineering
- No guarantee of complete source coverage
- No claim that an exposure record proves compromise
- No consumer-report use for regulated eligibility decisions
- No sensitive identifiers through the public website

Evidence handling

Reports are delivered through the client-approved secure channel. Evidence is minimized and masked where practical. Access, retention, authorized recipients, and destruction expectations are established in the agreement. This illustrative sample contains no real client, credential, victim, employee, or employer information.

Important limitation

External exposure intelligence is source-, scope-, and time-dependent. The absence of a finding does not prove the absence of exposure. Findings should be validated using client-side logs, identity systems, vendor information, and other authorized evidence.

THE DARKWATER PRODUCT

One useful report. Clear decisions. Optional monitoring.

The External Exposure Baseline is a paid, fixed-scope intelligence deliverable. It can stand alone or establish the verified foundation for ongoing Exposure Watch monitoring.

Baseline report

Risk-ranked findings, evidence notes, confidence, limitations, and a prioritized action register.

Priority notifications

Decision-ready alerts when a material finding meets the agreed escalation threshold.

Monthly intelligence brief

Material changes, false-positive reduction, action tracking, and clear no-change reporting.

NEXT STEP

Request a fixed-scope baseline without scheduling a sales call.

Begin with a company name, public domain, authorized business contact, and high-level objective. No passwords, confidential evidence, or personal executive identifiers are needed to begin.

darkwaterpi.com/start/

DarkWater Associates LLC
External Exposure Intelligence
Licensed North Carolina Investigations

Contact
(828) 540-0038
info@darkwaterpi.com