

PUBLIC SAMPLE / FICTIONAL ENGAGEMENT

# Cyber threat intelligence assessment

## Prepared for Northline Studio

A fictional organization used solely to demonstrate reporting. No client information, live indicators or actual evidence is included.

| Report reference | Reporting cutoff        | Intended reader                                  |
|------------------|-------------------------|--------------------------------------------------|
| CTI-001          | 07 Oct 2026 / 23:59 UTC | Security lead, SOC liaison and executive sponsor |

### EXECUTIVE ASSESSMENT

The fictional watch list contains two lookalike domains referencing payment support. Public records and a client-provided screenshot support a payment-redirection hypothesis, but do not establish a compromise, a named threat actor or data theft. A separate credential-exposure claim lacks source detail and is not treated as a verified leak.

### DECISION REQUESTED

Authorize the security team to validate the two reserved example indicators against its own telemetry. Do not automatically block, attribute or contact an alleged actor based on this sample.

## Inside this report

02 Scope and method / 03 Findings / 04 Evidence and chronology / 05 Action plan / 06 Handover and limitations

Illustrative format only. Final scope, response cadence, authorized recipients and local requirements are agreed for each engagement. No service outcome or legal determination is promised.

02 / HALDEN INTELLIGENCE

# Scope, coverage & method

AGREED QUESTION AND COVERAGE

Answer PIR-01: are public payment-themed references creating plausible exposure for the fictional client? Answer PIR-02: what evidence would justify an internal investigation? Review two domains, public page captures and one client-reported alert during 1-7 October.

OUTSIDE THIS ASSESSMENT

Buying stolen information, accessing private criminal forums, engaging threat actors, scanning third-party systems, handling raw credentials and continuous SOC monitoring.

| Asset / record               | Accountable owner | Coverage                                        |
|------------------------------|-------------------|-------------------------------------------------|
| AS-01 / Primary domain       | Security lead     | northline.example; reserved fictional domain    |
| AS-02 / Lookalike set        | Analyst           | pay-northline.example; northline-help.example   |
| AS-03 / Validation telemetry | Client SOC        | Not supplied at cutoff; explicit collection gap |

REPORTING METHOD

Define authority and scope; register supplied material; separate direct observations from statements; assess alternative explanations; review findings against source limitations; assign actions with acceptance evidence.

CONFIDENCE IS NOT SEVERITY

High: the cited material directly supports this narrow observation. Moderate: the observation has support but an important gap remains. Low: it is a lead or statement requiring corroboration. Confidence never establishes identity, intent or legal liability.

PRIORITY AND TIME

High: address promptly because of potential material harm or dependency. Medium: assign a near-term owner. Low: review in the agreed cycle. These are qualitative priorities, not CVSS ratings. All times are UTC; event times and receipt times are distinct.

## 03 / HALDEN INTELLIGENCE

# Findings & interpretation

## F-01 / HIGH PRIORITY / MODERATE CONFIDENCE

## Payment-redirection theme warrants validation

**Observation.** Two fictional page captures use the client's brand and payment-support language. Public domain observations are consistent with the listed references.

**Why it matters.** Users might be directed away from an official payment or support route.

**Alternative / uncertainty.** A training page, authorized agency or stale content could explain the observations; authorization must be checked.

**Recommended action.** Compare against approved domains and inspect permitted internal DNS or proxy telemetry before deciding containment.

Evidence: E-01, E-02

## F-02 / MEDIUM PRIORITY / LOW CONFIDENCE

## A common operator cannot be established

**Observation.** The captures share a layout and one phrase; no independent account, transaction or infrastructure linkage has been supplied.

**Why it matters.** Premature actor attribution could distort prioritization and external reporting.

**Alternative / uncertainty.** Independent reuse of a template is a credible explanation.

**Recommended action.** Track a shared theme only. State the additional corroboration needed before increasing confidence.

Evidence: E-02

## F-03 / MEDIUM PRIORITY / LOW CONFIDENCE

## Credential-exposure claim remains unverified

**Observation.** The fictional alert states that company credentials are exposed but provides no collection date, provenance or account-validation evidence.

**Why it matters.** The claim may require authorized identity-team checks, but does not establish usable credentials or access.

**Alternative / uncertainty.** The information could be stale, fabricated or unrelated to the client.

**Recommended action.** Ask for non-sensitive provenance and have the identity team inspect authorized signals. Do not request passwords or acquire a stolen dataset.

Evidence: E-03

04 / HALDEN INTELLIGENCE

# Evidence & chronology

## Evidence register

| ID / source                               | Receipt time (UTC)   | Known limitation                                  |
|-------------------------------------------|----------------------|---------------------------------------------------|
| E-01 / Fictional domain observation notes | 2026-10-02 10:00 UTC | Reserved example domains; no live query performed |
| E-02 / Fictional public page captures     | 2026-10-03 13:00 UTC | Content similarity is not identity attribution    |
| E-03 / Fictional client alert summary     | 2026-10-06 09:00 UTC | Single unverified claim; no credentials retained  |

## Event chronology

| Event time (UTC) | Recorded event                              | Source |
|------------------|---------------------------------------------|--------|
| 02 Oct / 10:00   | Two domain references entered in watch list | E-01   |
| 03 Oct / 13:00   | Payment narrative reviewed                  | E-02   |
| 06 Oct / 09:00   | Unverified alert added with low confidence  | E-03   |

HANDLING AND PROVENANCE

The entries above are invented descriptions, not evidence attachments. In a real engagement, assign a unique evidence ID; record collector, authority, source, collection and receipt times, method and limitations; retain the original in approved storage; and log access, transformations and transfers. Calculate digests on actual files where appropriate. Never invent a digest or custody event.

SOURCE BOUNDARIES

A screenshot can support what was visible in that copy. It does not, on its own, prove origin, completeness, authorship or the full history of an event. Preserve contradictions and distinguish client-reported events from independently verified observations.

05 / HALDEN INTELLIGENCE

# Action plan & service register

| When                  | Owner             | Completion evidence                                    | State           |
|-----------------------|-------------------|--------------------------------------------------------|-----------------|
| Next staffed review   | Security lead     | Confirm official domain inventory and authorization    | Open            |
| Within 1 business day | Client SOC        | Validate sample references against permitted telemetry | Awaiting client |
| Within 3 days         | Analyst           | Seek non-sensitive provenance for exposure claim       | Open            |
| Next briefing         | Executive sponsor | Review PIRs and agree collection gaps to address       | Planned         |

## Illustrative indicator register - do not deploy

| Reserved indicator     | Assessment                                   | Validation / expiry                               |
|------------------------|----------------------------------------------|---------------------------------------------------|
| pay-northline.example  | Fictional payment theme; moderate confidence | Owner check + internal telemetry; reassess 14 Oct |
| northline-help.example | Fictional support theme; moderate confidence | Check legitimate use before any control change    |
| 192.0.2.44             | Documentation-only IP; not an observed host  | Excluded from operational export                  |

All indicators are reserved examples, not actionable IOCs. A customer delivery would include provenance, first/last seen, confidence, expiration and sharing restrictions in an agreed format.

CLOSING AN ACTION

Record the actual completion time, responsible person and evidence reference. A request, recommendation or platform submission is not completion. Keep unresolved dependencies visible and agree the next review date with the client.

06 / HALDEN INTELLIGENCE

# Limitations & handover

LIMITS ON RELIANCE

No malware execution, endpoint evidence or internal telemetry was reviewed. No named actor, confirmed intrusion or exfiltration conclusion is supported.

DISTRIBUTION AND RETENTION

This fictional sample is public. A live report requires an approved recipient list, secure delivery method, retention schedule and disposal owner agreed with the client and, where relevant, counsel. Do not place real evidence or personal data in public website assets.

## Release checklist for a live engagement

| Required check          | Record to complete before issue                            |
|-------------------------|------------------------------------------------------------|
| Authority and scope     | Approved instruction reference and authorized assets       |
| Analyst and peer review | Named preparer, reviewer, review date and corrections      |
| Client decisions        | Decision owner, accepted actions and unresolved objections |
| Delivery and acceptance | Approved recipients, transfer receipt and acceptance date  |
| Follow-up and retention | Next review, retention basis and disposal responsibility   |

These fields are deliberately unsigned. No real review, instruction, client approval or evidence transfer is represented by this sample.

## Method references

Background guidance only; these publications do not validate fictional findings or certify this report. Apply current platform procedures and engagement-specific legal advice separately.

NIST SP 800-61 Rev. 3 — Incident Response Recommendations and Considerations for Cybersecurity Risk Management (2025)  
<https://csrc.nist.gov/pubs/sp/800/61/r3/final>

FIRST — Traffic Light Protocol, version 2.0  
<https://www.first.org/tlp/>