CYBERINTEL.PRO

ANONYMISED ENGAGEMENT RESULTS

Results From Real Engagements

Four completed intelligence engagements — situations, evidence, assessed business impact and delivered outcomes.

4	16	15	3
engagements documented	findings detailed	evidence exhibits	continents covered

ILLUSTRATIVE SAMPLE — NOT A CLIENT DELIVERABLE

Karen Shahbazian
Independent Cyber Intelligence Consultant

cyberintel.pro
contact@cyberintel.pro

Contents

This document sets out four completed engagements in full: what the client faced, what was found, what each finding meant commercially, and what changed as a result.

SECTION 01

Executive summary

Four engagements, conducted between 2023 and 2025 across Europe, Israel and the United Kingdom. Every client detail has been removed or altered. Findings, severities, evidence structures and outcomes are drawn from the actual work.

16
findings across four engagements

9
rated Critical

4/4
clients acted on the findings

0
findings disputed by clients

The engagements collected here have little in common on the surface. One concerns a founder's personal exposure ahead of a public listing. One is an external infrastructure review for a fintech platform mid-fundraise. One is an attribution assessment for a manufacturer that had been broken into three times. One is a due-diligence investigation for a private equity firm about to sign.

What they share is the shape of the problem. In each case the client had already done the obvious things — background checks, a security engineer, an MSSP, standard diligence — and in each case something material sat outside the boundary of what those measures were built to see. Not because the measures were poor, but because they were scoped to a definition of the perimeter that no longer matched where the risk actually lived.

Three patterns account for most of what follows. First, the highest-severity findings almost never involved a technical exploit; they involved something that had been left behind, forgotten, or never inventoried. Second, in three of four engagements the decisive evidence existed only outside English-language sources or outside the client's own estate. Third, the commercial consequence of a finding was consistently larger than its technical severity would suggest — a forgotten development server is a low-effort finding that happened to hold the production signing key.

Engagements at a glance

#	ENGAGEMENT TYPE	CLIENT PROFILE	FINDINGS	SEVERITY MIX	OUTCOME
01	Executive Digital Exposure	Pre-IPO technology founder	5	2 Critical · 2 High · 1 Medium	Listing proceeded on schedule
02	External Attack Surface	Fintech platform, Series B	4	2 Critical · 2 High	Round closed, no security findings raised
03	Threat Actor Attribution	European engineering manufacturer	4	2 Critical · 2 High	Attribution accepted as expert evidence

#	ENGAGEMENT TYPE	CLIENT PROFILE	FINDINGS	SEVERITY MIX	OUTCOME
04	Financial-Sector Investigation	Private equity, secondary transaction	3	2 Critical · 1 High	Transaction restructured before signing

THE RECURRING CONCLUSION

In all four engagements the client's existing controls were competent and the people running them were capable. The gap was not diligence — it was field of view. Each finding sat in a place nobody had been asked to look: a broker database, a lapsed vendor DNS record, a certificate reused by an operator, a registry entry filed under a different transliteration of the same name.

SECTION 02

Methodology and assurance

All work is conducted from open, commercial and closed-community sources. No engagement involves unauthorised access to any system, account or network.

Collection standards

Every engagement proceeds from a written scope agreed in advance and signed by the client. Collection is passive by default: public records, corporate and property registries, court and regulatory filings, breach corpora held under commercial licence, certificate transparency logs, passive DNS, code-hosting platforms, and monitored closed forums where access is established and maintained lawfully.

Where a finding requires confirmation that a service is live, verification is limited to the minimum interaction that establishes the fact — an unauthenticated HTTP request to a public endpoint, a DNS resolution, a TLS handshake. No credential is ever submitted. No authentication is ever attempted, including with credentials recovered during the engagement. Where a recovered credential appears to be live, that assessment is stated as an inference from format and reuse patterns, never from a login attempt.

Handling and disclosure

Recovered credentials, personal data and privileged material are held encrypted for the duration of the engagement and destroyed on delivery unless the client instructs otherwise in writing. Where collection touches third parties — family members, colleagues, counterparties — only material relevant to the agreed scope is retained.

Findings that indicate a live, exploitable exposure are reported to the client immediately on discovery rather than held for the final report. In two of the four engagements documented here, the client was notified of a Critical finding within hours of it being confirmed.

Analytic tradecraft

Assessments distinguish between what was observed and what is inferred from it. Observed facts are stated plainly. Inferences carry an explicit confidence level and the reasoning that supports them. Where an alternative explanation for the evidence is plausible, it is stated alongside the primary assessment rather than omitted.

Attribution work in particular is held to a higher standard: a single shared indicator is treated as a lead, not a conclusion. The assessment in Engagement 03 rests on infrastructure reuse, tradecraft concordance and independent motive evidence converging, and it says so.

Independence

Engagements are delivered personally by Karen Shahbazian or under direct supervision. There is no subcontracting of analysis to third parties, no reseller relationship with any tooling or monitoring vendor, and no commission arrangement on any remediation recommended. Where a recommendation names a category of product or service, the client is told that the recommendation carries no commercial interest.

SECTION 03

Severity and confidence framework

Severity describes commercial consequence, not technical novelty. A trivially discovered exposure that hands over a production key is Critical; an elegant finding with no realistic path to harm is not.

Severity ratings

RATING	DEFINITION	IN THIS DOCUMENT
CRITICAL	Direct, presently available path to material financial loss, regulatory exposure, physical risk to a person, or loss of the asset the business is built on. Action expected within days.	**9 of 16**
HIGH	Substantial harm requires one additional step or one plausible assumption. The exposure is real and the path is clear, but not yet complete. Action expected within weeks.	**6 of 16**
MEDIUM	Meaningful contribution to attacker capability, or a genuine exposure whose realistic harm is bounded. Action expected within the current quarter.	**1 of 16**
INFORMATIONAL	No present harm; recorded because it establishes context, or because a change in circumstances would make it material.	**0 of 16**

Confidence language

Confidence is stated separately from severity, because a finding can be severe and uncertain, or minor and definite. Three levels are used and they are used consistently.

LEVEL	WHAT IT MEANS
High confidence	Multiple independent sources agree, or a single source is directly verifiable and was verified. Alternative explanations were considered and do not fit the evidence.
Moderate confidence	The evidence supports the assessment and no contrary evidence was found, but corroboration is partial or the source set is narrow.
Low confidence	The assessment is plausible and worth acting on as a precaution, but the evidence would not withstand challenge. Stated as such.

What severity deliberately excludes

Severity is not adjusted for how difficult the finding was to make, how sophisticated the responsible party appears, or how embarrassing the finding is to the client. Several of the Critical findings in this document took under an hour to establish. That is a property of the exposure, not a reason to downgrade it — an exposure that is cheap to find is one that others will also have found.

SECTION 04 · EXECUTIVE DIGITAL EXPOSURE

Pre-IPO founder exposure assessment

A founder six months from a public listing, with no visibility into what an interested party could assemble about her from public sources alone.

Engagement profile

Subject	Founder and chief executive, technology company
Sector and geography	Enterprise software · Western Europe, operations in three countries
Commercial context	Approximately six months from an initial public offering
Engagement driver	Anticipated press attention, investor scrutiny and elevated personal profile
Scope	Personal digital exposure of the subject and immediate household; no corporate infrastructure
Duration	Three weeks, followed by a twelve-month monitoring retainer
Deliverable	Written assessment, prioritised remediation plan, executed takedown programme

Situation

The subject came to the engagement with a specific and well-framed concern. She was about to become considerably more visible: an IPO brings press profiles, analyst attention, activist interest and, for a founder with a personal story, a degree of public identification that does not reverse. She wanted to know what an interested party — a journalist, a short-seller, a hostile competitor, or someone with a personal grievance — could assemble about her without breaking any law.

She had taken the precautions a careful person takes. Social accounts were set to private. She used a password manager. She had never been the subject of a public incident. Her assumption, reasonable on its face, was that the assessment would return a short list of minor items.

The assessment returned five findings, two of them Critical. None of them required a technical compromise of anything she owned. All five were assembled from sources that were open to anyone willing to spend an afternoon looking, and the most serious of them had been sitting in place, unnoticed, for four months.

Findings summary

ID	FINDING	SEVERITY	IMPACT DOMAIN
EDE-01	Residential address and personal telephone number aggregated across three data broker platforms	CRITICAL	Physical security · Household
EDE-02	Personal email credentials recoverable from two breach corpora with a derivable password rule	CRITICAL	Account takeover · Financial
EDE-03	Active impersonation account operating undetected against the subject's genuine network	HIGH	Fraud · Reputation · Deal integrity
EDE-04	Household movement pattern derivable from tagged social media over a twenty-six week window	HIGH	Physical security · Family safety
EDE-05	Domain registered in the subject's legal name by an unidentified third party	MEDIUM	Impersonation · Business email compromise

EDE-01

Residential address and personal telephone aggregated across three data broker platforms

CRITICAL Confidence: High · Source: Commercial people-search aggregators · Verified by independent retrieval

EVIDENCE

Exhibit EDE-01. Aggregated broker records returning the subject's residential address, personal telephone number and cross-referenced relatives. Precise values redacted for publication.

ASSESSMENT

Three commercial people-search platforms held a current residential address for the subject, two held a personal mobile number in active use, and all three published a list of cross-referenced relatives. Two of the three published an exact date of birth. The records were retrieved independently and matched each other, which rules out a single stale source propagating an old entry.

The address was current, not historical. It corresponded to the property the subject had moved to eighteen months earlier and had never publicly associated with her name. The most likely origin is a property transaction record combined with a utility or electoral data supply — routine commercial data flows, aggregated into something the subject had never consented to and did not know existed.

BUSINESS IMPACT

The exposure is a physical security matter first and a privacy matter second. A verified home address paired with a working mobile number and a list of family members is the standard input set for targeted harassment, for doorstepping by press, and for the household-level pretexting that precedes a serious social-engineering attempt. The listing was the aggravating factor: the subject's profile was about to rise sharply and permanently, and these records were indexed and waiting.

There is a second-order commercial consequence that clients often miss. An executive who becomes the subject of a physical security incident during a listing process creates a disclosure question, a board question and a press question simultaneously, at the exact moment the company can least absorb any of them. The cost of the exposure is not bounded by the harm to the individual.

The relatives listing compounds the problem materially. Family members had not consented to the subject's public profile and had none of her security awareness, yet they were reachable, named and locatable. In practice, the family is the softer route to the principal.

REMEDIATION DELIVERED

Formal opt-out and suppression requests filed with all three platforms, tracked to completion rather than submitted and assumed. Two required manual identity verification and took thirty and forty-five days respectively.

Upstream data supply identified and suppressed where the legal basis permitted, to prevent the records repopulating — the failure mode that defeats most self-service removals.

Personal mobile number retired and replaced with a number held under a service entity rather than the subject's name.

Quarterly re-checks added to the monitoring retainer, on the basis that broker records reappear after roughly nine to fifteen months without ongoing suppression.

EDE-02

Personal email credentials recoverable from two breach corpora with a derivable password rule

CRITICAL Confidence: High · Source: Licensed breach corpora · No authentication attempted at any point

EVIDENCE

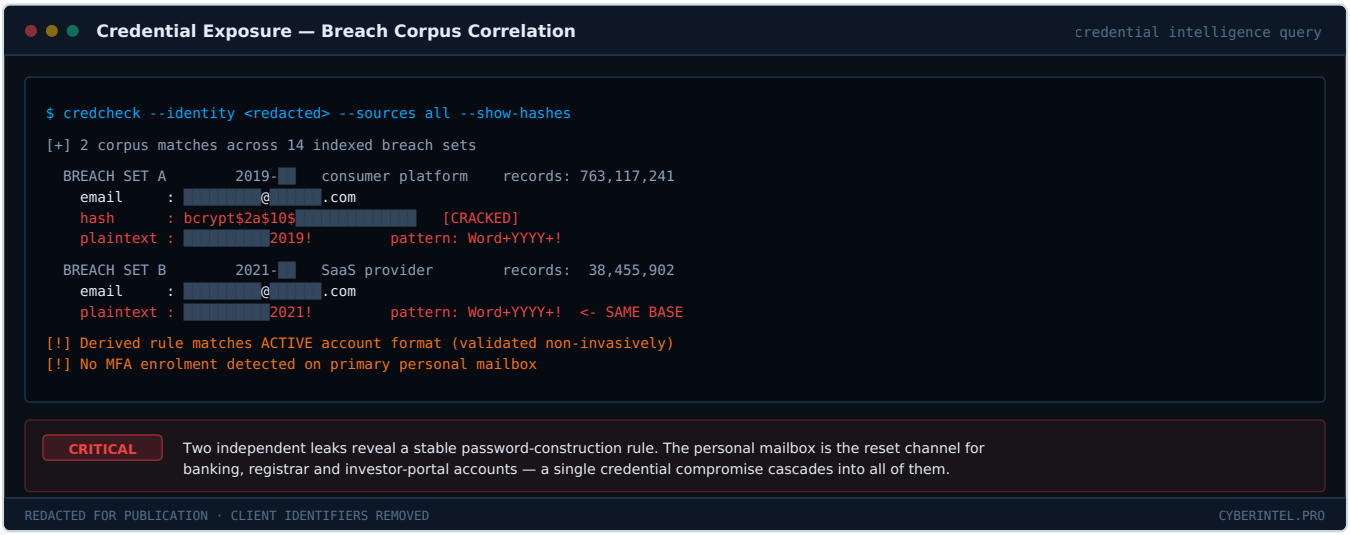

Exhibit EDE-02. Correlation across two breach sets exposing a consistent password-construction rule. Hashes and plaintext redacted; no credential was ever submitted to any service.

ASSESSMENT

The subject's personal email address appeared in two indexed breach corpora, from unrelated services, four years apart. In both cases the password was recoverable — in one from a cracked bcrypt hash, in the other from a plaintext dump. Neither password was the same. Both followed an identical construction rule: a fixed base word, the year of the account's creation, and a terminal exclamation mark.

This is the finding that matters, and it is not the leaked passwords themselves. Both are long since changed. What leaked was the subject's method — and a method persists across every password a person generates by hand. Given the rule and a target year, the candidate space for any hand-made password on any account collapses from impractical to trivial.

The affected mailbox was the subject's primary personal address and the registered recovery channel for personal banking, the domain registrar holding her personal domains, two brokerage accounts and — critically — the investor relations portal being used in the listing process. No multi-factor authentication was enrolled on it. This is stated at high confidence from enrolment metadata; it was not tested by attempting to sign in.

BUSINESS IMPACT

The realistic worst case is not the loss of an email account. It is a chain: the mailbox is compromised using a password derived from the known rule, and every service that treats that mailbox as the reset channel becomes reachable in sequence. Banking, brokerage, registrar and the investor portal all fall inside that chain. The absence of a second factor removes the only control that would interrupt it.

The investor relations portal deserves separate weight. During a live listing process, an actor with mailbox access has visibility into deal correspondence, draft disclosures and analyst communications — material that is price-sensitive by definition. The exposure is therefore not solely a fraud risk to the individual; it is a market-integrity and regulatory-disclosure risk to the company, and the company had no visibility into it because the account was personal.

The password rule finding also invalidates a control the subject believed she had. She used a password manager, and reasonably regarded that as sufficient. But the manager held generated passwords for newer accounts, while older and personally memorable accounts retained hand-made passwords built on the exposed rule. The control was real; its coverage was partial, and the gap was exactly where the value sat.

REMEDIATION DELIVERED

Full credential rotation across every account traceable to the exposed address, prioritised by the reset-chain dependency rather than by account age.

Hardware-token multi-factor authentication enrolled on the primary mailbox, banking, brokerage and the investor portal. Application-based factors used where hardware tokens were unsupported.

Recovery-channel architecture redesigned: the personal mailbox was removed as the reset path for financial and corporate accounts and replaced with a dedicated address not published anywhere and not used for correspondence.

Every remaining hand-made password identified and replaced with generated values, closing the coverage gap in the password manager rather than assuming it.

EDE-03

Active impersonation account operating undetected against the subject's genuine network

HIGH Confidence: High · Source: Professional platform enumeration · Corroborated with the subject's own contacts

EVIDENCE

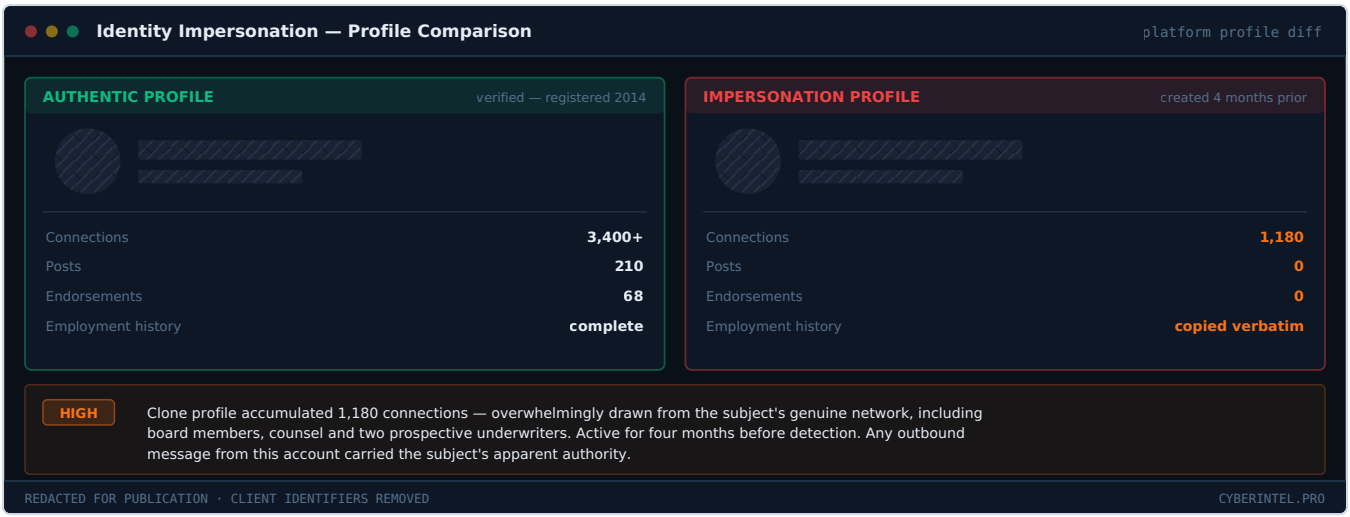

Exhibit EDE-03. Authentic and impersonation profiles side by side. The clone reproduced employment history verbatim and had accumulated 1,180 connections from the subject's genuine network.

ASSESSMENT

A second profile existed on a major professional platform using the subject's name, photograph and employment history, the latter copied verbatim. It had been created four months before the engagement began. In that period it had accumulated 1,180 connections and had never posted any content — a profile built for reach, not for visibility.

Analysis of the connection set was the decisive step. The connections were not random: they were disproportionately drawn from the subject's genuine professional network, including current and former colleagues, two board members, the company's external counsel, and individuals at two institutions involved in the listing. Whoever built the profile had worked from the subject's real network and targeted it deliberately.

No fraudulent message from the account was recovered, and the client was told so plainly. The absence of recovered messages is not evidence that none were sent; direct messages on the platform are not observable to an external party. The finding is scoped to what was established: the account existed, it was targeted, and it had four months of unmonitored access to the subject's professional circle.

BUSINESS IMPACT

The value of an impersonation account is borrowed authority. A message from a founder to a colleague, a board member or an underwriter carries an implicit weight that a stranger's message never will. Requests that would prompt verification from an unknown sender — an introduction, a document, a change of payment detail, a quiet question about deal timing — are routinely actioned when they appear to come from the principal.

The timing is the aggravating factor. The account was created four months before a listing, and connected to counsel and underwriters. That pattern is consistent with preparation for a specific, timed action rather than with generic profile-farming. The plausible objectives range from harvesting non-public deal information to attempting a payment-redirection fraud at closing, when transfer volumes are high and unusual instructions attract less friction.

Reputational exposure runs alongside the fraud exposure and is harder to contain. Statements or approaches made under the subject's name to people whose opinion determines the success of a listing cannot be fully retracted once made — a correction reaches a fraction of the audience that the original reached.

REMEDIATION DELIVERED

Platform escalation filed through the impersonation channel with a full evidence package. Account removed within forty-eight hours.

Full connection set of the fraudulent profile extracted and preserved before takedown, so that the exposed population was known rather than assumed.

Direct notification to the highest-risk contacts — board, counsel, underwriters — advising that any approach from the subject in the preceding four months should be reconfirmed through a known channel.

Continuous impersonation monitoring across the major professional and social platforms added to the retainer, with a defined escalation path so future clones are addressed in days rather than months.

EDE-04

Household movement pattern derivable from tagged social media over a twenty-six week window

HIGH Confidence: High · Source: Public social metadata, third-party tagging · Subject's own accounts were private

EVIDENCE

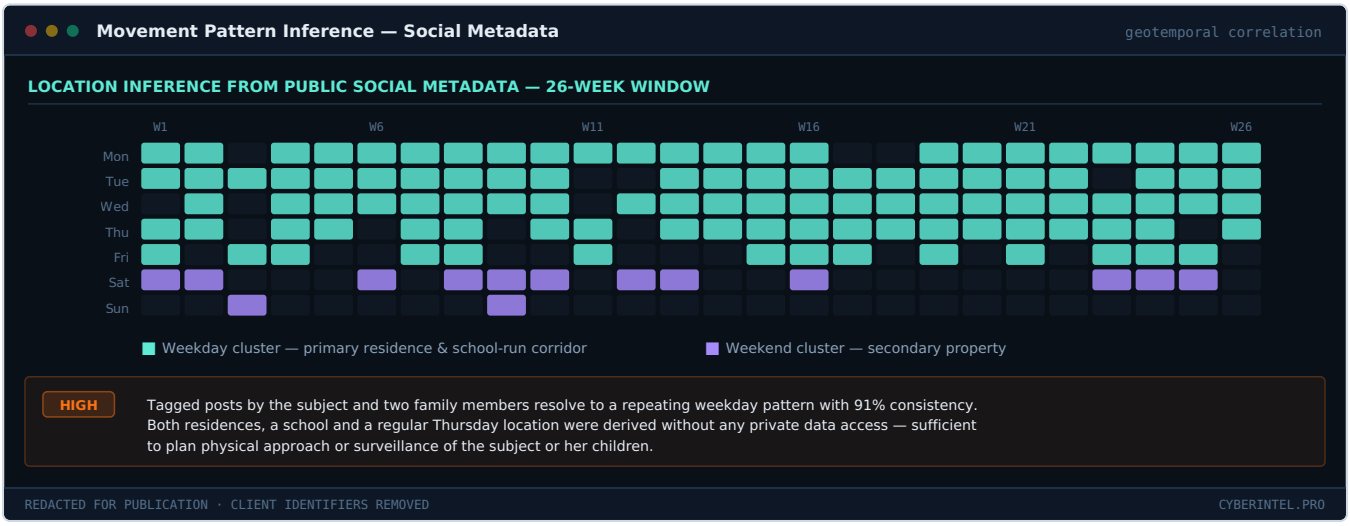

Exhibit EDE-04. Twenty-six weeks of tagged public posts resolved into a repeating weekly location pattern. Both residences, a school and a fixed weekly commitment were derived without any private data access.

ASSESSMENT

The subject's own social accounts were private and well managed. The exposure came entirely from other people: two family members with public accounts who tagged the subject, tagged locations, and posted on a predictable rhythm. Twenty-six weeks of that material, aggregated, resolved into a weekly pattern with ninety-one per cent consistency.

What the pattern yielded was specific: the primary residence, a secondary property used at weekends, the school attended by the subject's children including arrival and departure windows, and a fixed Thursday commitment at a consistent location and time. None of this was stated anywhere. All of it was derivable.

This finding is worth isolating because it defeats the most common executive-protection assumption. The subject had done everything correctly with her own accounts. Her exposure was created by people who love her, acting entirely normally, with no awareness that their posts aggregated into a surveillance product.

BUSINESS IMPACT

A reliable weekly movement pattern is the operational prerequisite for physical approach. It converts an intention to reach someone into a plan with a time and a place. Combined with the residential address from EDE-01, the subject's household was locatable and her routine predictable — the two inputs that matter for harassment, for confrontation, and for anything more serious.

The child-related exposure is the most serious element in this engagement and was treated as such. School location with timing windows, associated with a named parent whose public profile was about to rise sharply, is a category of exposure that does not admit a proportionate commercial framing.

> There is also a straightforward professional consequence. A derivable calendar reveals commercial activity: a recurring weekday location near an institution the company was in confidential discussions with was visible in the pattern. Movement data leaks deal information even when nobody involved says anything.

REMEDIATION DELIVERED

> Historical tagged content audited and, where the family agreed, removed or de-tagged, prioritising posts that established the pattern rather than attempting comprehensive deletion.
>
> Direct briefing delivered to household members — framed as a practical explanation of how aggregation works rather than as a list of prohibitions, on the basis that rules people understand are the only ones that survive.
>
> Platform-level tagging permissions reconfigured so that the subject's association with third-party content requires approval.
>
> Physical security review of both properties and the school route recommended and referred to a specialist provider, with no commercial relationship to this engagement.

EDE-05

Domain registered in the subject's legal name by an unidentified third party

MEDIUM Confidence: Moderate on intent, High on the facts · Source: Registry and passive DNS

EVIDENCE

Exhibit EDE-05. Registry record showing the subject's legal name as registrant, with functioning mail exchange records and no sender authentication configured.

ASSESSMENT

A domain closely matching the subject's legal name had been registered fourteen months previously through an offshore, privacy-forward registrar. The subject's name appeared in the registrant field. She had no knowledge of it and had not authorised it.

The web presence was inert — a registrar parking page. The mail configuration was not. Mail exchange records were configured and answering, meaning the domain could send and receive email. Neither SPF nor DMARC was present, so nothing constrained what could be sent from it.

Intent could not be established and the assessment says so. Three explanations fit the evidence: speculative registration by a domain investor anticipating the listing; a defensive registration by a third party with no malicious purpose; or a pre-positioned asset acquired ahead of a planned impersonation. The rating is Medium because harm requires a further action, not because the finding is benign. Read alongside EDE-03, the third explanation is the one that warranted planning against.

BUSINESS IMPACT

An email arriving from a domain that reads as the subject's own name passes the recipient's first credibility test before its content is considered. During a listing, when correspondence volume rises and counterparties multiply, the population of recipients who would accept such a domain as legitimate is at its largest.

The specific exposure is business email compromise timed to closing. Payment instructions, document requests or timing enquiries sent from a name-matching domain to counsel, underwriters or the finance function are difficult to distinguish from genuine correspondence, particularly under transaction pressure. The absence of SPF and DMARC means no technical control would flag them.

There is a lower-probability but higher-impact variant worth noting: the same asset could be used to publish or distribute statements in the subject's name at a moment when market-sensitive information is in play. The commercial consequence of that during an offer period is disproportionate to the trivial cost of holding the domain.

REMEDIATION DELIVERED

Domain acquired through an intermediary, at a cost that did not warrant the alternative of a formal dispute process taking months.

Sender authentication configured on the acquired domain — SPF, DKIM and a DMARC reject policy — so it cannot be used to send even if control is later lost.

Defensive registration extended across the obvious variants of the subject's name and the principal top-level domains, an inexpensive measure relative to the exposure it closes.

Registry monitoring for new registrations matching the subject's name or the company's marks added to the retainer.

OUTCOME

All three data broker listings were removed and confirmed removed, with upstream suppression filed to prevent repopulation. The impersonation account was taken down within forty-eight hours of escalation, and its full connection set was preserved beforehand so that the exposed population was known rather than estimated. Credentials were rotated across the reset chain and hardware multi-factor authentication was enforced on every account in it. The unauthorised domain was acquired, secured and authenticated.

The subject completed the listing process on schedule. No security incident occurred during the offer period. The twelve-month monitoring retainer detected and resolved two further impersonation attempts in the nine months following the listing — both within days of appearing, rather than the four months the original clone had run undetected.

Value delivered

5
findings, from zero known at engagement start

48h
to remove an account active for four months

100%
of broker listings removed and suppressed

0
incidents during the offer period

SECTION 05 · EXTERNAL ATTACK SURFACE

Fintech platform, Series B due diligence

A company with a full-time security engineer, a clean posture on paper, and three internet-facing servers nobody remembered building.

Engagement profile

Client	Venture-backed payments and lending platform
Sector and geography	Financial technology · Northern Europe, regulated entity
Scale	123 employees · approximately 40,000 end customers
Commercial context	Series B fundraise, lead investor technical due diligence pending
Engagement driver	Independent external validation ahead of investor review
Scope	Everything reachable from the public internet, plus workforce credential exposure
Duration	Two weeks to report; critical findings escalated on discovery

Situation

The client was a well-run company by any reasonable measure. It employed a full-time security engineer, ran an established vulnerability management process, held the certifications its regulator expected, and had passed penetration tests. The engagement was commissioned as a confirmatory exercise: the lead investor's technical due diligence was scheduled, and management wanted an independent view first so that anything found would be found by them rather than by the investor.

Management's expectation, stated at kick-off, was that the assessment would surface housekeeping items. This was not unreasonable. Their internal view of the external estate was accurate as far as it went, and everything inside that view was well maintained.

The assessment produced four findings, two Critical. The determining factor in all four was the same: they concerned assets the company did not know it owned, or exposures that existed in places the company had no mandate to look. The security engineer had secured the estate as it was documented. The estate as it actually existed was larger.

Findings summary

ID	FINDING	SEVERITY	IMPACT DOMAIN
EAS-01	Three undocumented development servers internet-facing, two exposing production secrets	CRITICAL	Full platform compromise · Funds

ID	FINDING	SEVERITY	IMPACT DOMAIN
EAS-02	Forty-seven workforce credentials in public breach corpora, eleven matching current policy	CRITICAL	Account takeover · Treasury fraud
EAS-03	Wildcard DNS delegation to a decommissioned vendor serving a live branded login page	HIGH	Credential harvesting · Customer trust
EAS-04	Internal architecture and operations documentation in a former contractor's public repository	HIGH	Reconnaissance uplift · Social engineering

EAS-01

Three undocumented development servers internet-facing, two exposing live production secrets

CRITICAL Confidence: High · Source: Passive enumeration, verified by unauthenticated retrieval · Escalated within four hours

EVIDENCE

Exhibit EAS-01. Enumeration output and the retrieved configuration file. Production payment keys, database credentials and the JWT signing key were readable without authentication.

ASSESSMENT

Passive enumeration identified three live hosts under the client's domain that did not appear in the asset inventory: a development API server, a staging environment and a build host. All three were reachable from the public internet. All three had been running continuously for a period the client could not determine, because nothing was monitoring them.

Two exposed configuration endpoints without authentication. A single unauthenticated HTTP request to the development API host returned an environment file containing a live payment-processor secret key, the hostname and credentials for the production database cluster, the production JWT signing key, and a transactional email provider key.

The critical detail is that these were production values in a development environment. The environment file had been copied from production during a migration, and the host was left running when the work concluded. No exploit was involved at any stage. The material was served, on request, to anyone who asked.

BUSINESS IMPACT

This finding placed the entire platform at risk of takeover, and the JWT signing key is the reason. Possession of the signing key allows an actor to mint valid authentication tokens for any user, including administrative users, without ever touching a login form. There is no credential to steal, no factor to bypass, and no failed-login signal to detect. Every subsequent action appears to the platform as a correctly authenticated session.

The payment-processor key permits transactions and refunds against a live account. For a payments company, that is direct financial loss with an immediate customer-facing dimension. The database credentials expose the full customer record set — for a regulated financial entity in this jurisdiction, a confirmed breach of that data carries mandatory regulatory notification, customer notification, and a penalty exposure calculated against global turnover.

The commercial consequence extended to the transaction in progress. Had the lead investor's technical due diligence identified this finding rather than the client, the reasonable outcomes range from a valuation adjustment through an extended diligence period to a withdrawn term sheet. Investor confidence in a payments business rests substantially on the credibility of its engineering discipline, and a production signing key served unauthenticated from a forgotten host is difficult to characterise as a housekeeping oversight.

It is worth stating what this finding says about the internal process, because the client asked. The security engineer was competent and the vulnerability management programme was functioning. Neither could act on hosts that were not in the inventory. The failure was not in the security function; it was in the absence of any process that reconciled what the inventory claimed against what the internet could actually see.

REMEDIATION DELIVERED

Client notified within four hours of confirmation, ahead of any written deliverable. All three hosts were taken offline the same day.

Every exposed secret rotated within twenty-four hours: payment-processor key, database credentials, JWT signing key and email provider key. Signing key rotation forced a full session invalidation across the platform, which was accepted as the correct trade.

Retrospective log review commissioned across the exposure window to establish whether the material had been retrieved by any other party. No evidence of malicious retrieval was identified, though log retention did not cover the full period — a limitation stated plainly rather than presented as an all-clear.

Continuous external asset discovery implemented, reconciling observed internet-facing hosts against the inventory rather than relying on the inventory alone. This closed the class of finding, not merely the instance.

EAS-02

Forty-seven workforce credentials in public breach corpora, eleven matching current password policy

CRITICAL Confidence: High · Source: Licensed breach corpora correlated against public directory data · No authentication attempted

EVIDENCE

Exhibit EAS-02. Workforce credential exposure by function. Eleven recovered passwords conform to the organisation's current complexity policy, indicating plausible live credentials rather than stale ones.

ASSESSMENT

Forty-seven corporate email addresses appeared in public breach corpora with recoverable passwords — thirty-eight per cent of the workforce. Volume alone would be unremarkable; a company of this size will always have some historical exposure.

The material finding is the subset. Eleven of the forty-seven recovered passwords conform to the organisation's current Active Directory complexity policy: correct length, correct character-class composition, consistent with the format staff are presently required to use. Passwords predating the current policy would not satisfy it. These do, which makes them plausible live credentials rather than historical artefacts.

Distribution mattered more than the total. Exposure was concentrated in Finance and Treasury at seventy-three per cent, and in the Executive and Board group at fifty-six per cent — the two populations holding payment authority and the highest-value access. Thirteen of the exposed accounts carried privileged access of some form. This is stated as an inference from format matching and directory metadata; no login was attempted with any recovered credential.

BUSINESS IMPACT

For a payments company, the treasury exposure is the sharp end. An actor holding a working credential for a finance function with payment authority does not need to defeat the platform's security; they need only operate within it as an authorised user. Payment fraud executed through legitimate credentials is materially harder to detect than intrusion, because every control the transaction passes through returns a correct result.

The eleven policy-matching credentials also indicate a behavioural pattern rather than eleven isolated mistakes. Staff who reuse a work password on an external service that is later breached will, in general, do so again. The finding therefore describes a recurring condition, not a one-off event, and remediation had to address the behaviour as well as the eleven accounts.

Regulatory exposure applies independently of whether a compromise occurred. As a regulated entity, the client is expected to demonstrate credential hygiene commensurate with the risk it carries. A supervisory review that identified thirty-eight per cent workforce exposure with concentration in treasury would be difficult to answer, whatever the incident history.

In the investor context, this finding was second only to EAS-01 in significance. It is the kind of exposure a technical diligence team looks for specifically, because it is cheap to check and highly diagnostic of internal discipline.

REMEDIATION DELIVERED

Forced password reset across all forty-seven affected accounts, with the eleven policy-matching accounts reset within hours of notification and the remainder within the working week.

Multi-factor authentication enforced across the full workforce, having previously been enforced only for privileged accounts — the change that most reduced the exploitability of any future exposure.

Breach-corpus monitoring implemented against the corporate domain with automated alerting, so that new appearances are detected in days rather than at the next assessment.

Targeted briefing for the Finance and Treasury function specifically, addressing password reuse as a treasury-control matter rather than as a general IT topic, which is how it had previously been framed and ignored.

EAS-03

Wildcard DNS delegation to a decommissioned vendor serving a live branded login page

HIGH Confidence: High · Source: DNS resolution and unauthenticated HTTP inspection

EVIDENCE

Exhibit EAS-03. Resolution chain from the client's domain through a wildcard CNAME to infrastructure the client no longer controls, terminating in a functional branded login form.

ASSESSMENT

A wildcard CNAME record under the client's primary domain delegated to a third-party vendor platform. The vendor relationship had ended more than two years previously. The DNS record was never withdrawn.

The delegated infrastructure was still answering. It returned a functional login page carrying the client's branding, served over HTTPS with a valid certificate for the client's own domain, and set a session cookie. To any visitor, and to most automated checks, it was indistinguishable from a genuine client property.

The wildcard is what elevates this from a stale record to a systemic exposure. Because the delegation is a wildcard, any hostname under the client's domain that is not explicitly defined resolves to third-party-controlled infrastructure. The exposure is not one hostname; it is the entire unallocated namespace.

BUSINESS IMPACT

The client's own domain, with a valid certificate, presenting a login form the client does not control, is the most credible phishing infrastructure that could be constructed against its customers — and it does not need to be constructed, because it already exists. Every indicator a security-aware customer is taught to check returns a correct result: the domain is right, the certificate is valid, the branding is genuine.

Detection from the client's side would be near-impossible. Credentials submitted to that page never reach the client's systems, so there is no failed-login telemetry, no anomalous traffic and no log entry anywhere in the client's estate. The first indication would be downstream fraud whose origin could not be traced back.

Because the vendor account is now under unknown control, the exposure is not theoretical dormancy. Whoever holds that account can change what the page does at any time, without touching anything the client owns or monitors. For a regulated financial platform, a credential-harvesting page operating under its own domain is both a customer-harm event and a supervisory matter.

REMEDIATION DELIVERED

Wildcard record withdrawn immediately and replaced with explicit records for defined hostnames only, eliminating the unallocated-namespace exposure.

Full DNS zone audit conducted across all client domains, identifying and removing four further delegations to services no longer in use. This was the class-level fix.

Certificate transparency monitoring implemented so that certificates issued for the client's domains by any party generate an alert.

DNS record lifecycle tied to vendor offboarding in the procurement process, so that contract termination triggers a delegation review rather than relying on someone remembering.

EAS-04

Internal architecture and operations documentation in a former contractor's public repository

HIGH Confidence: High · Source: Code-hosting platform reconnaissance · Publicly indexed for approximately fourteen months

EVIDENCE

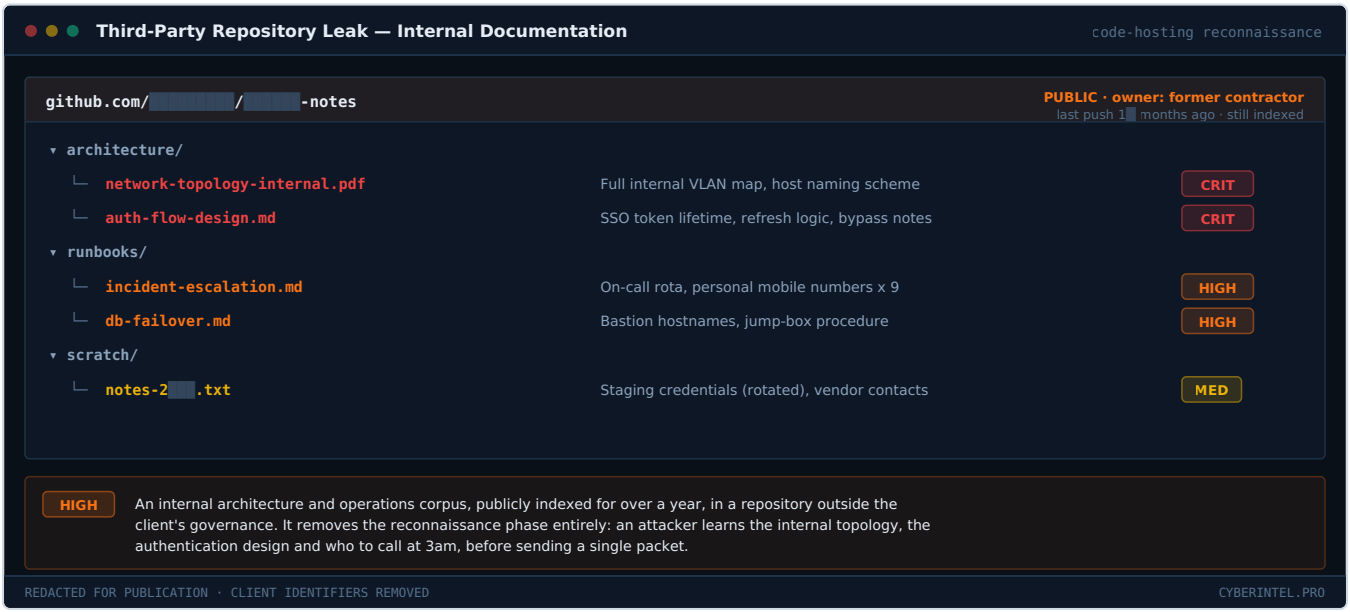

Exhibit EAS-04. Public repository owned by a former contractor containing internal network topology, authentication design and operational runbooks with named on-call contacts.

ASSESSMENT

A public repository belonging to a contractor who had left the engagement more than a year earlier contained a working copy of internal documentation. It had been publicly indexed for approximately fourteen months and sat entirely outside the client's governance — the client had no visibility into it and no authority over it.

The contents were substantive rather than incidental. Internal network topology including VLAN structure and host naming conventions. Authentication flow design covering single sign-on token lifetimes, refresh logic and known bypass conditions. Operational runbooks with the on-call rota, nine personal mobile numbers, bastion hostnames and jump-box procedures. A scratch file with staging credentials, since rotated.

No production credential was live at the time of discovery. That is the reason the finding is High rather than Critical, and it is close to the boundary.

BUSINESS IMPACT

The value of this material to an attacker is that it removes reconnaissance. Internal topology, naming conventions and authentication design are precisely what an intruder would otherwise spend weeks establishing after gaining a foothold — noisily, with a meaningful chance of detection. Supplied in advance, an actor can plan a route to the target before sending a single packet, and execute it with far less interaction than detection controls are tuned to catch.

The authentication design material is the most damaging single element. Token lifetimes, refresh behaviour and documented bypass conditions describe where the design is soft. That is a map to the weakest point in the client's access control, written by people who understood it well.

The operational runbooks create a distinct social-engineering exposure. An actor who knows the on-call rota, has the on-call engineer's personal mobile number, and can reference genuine internal hostnames and correct escalation procedure is well positioned for a pretext call — particularly out of hours, when the recipient is tired and the request sounds procedurally correct. Every detail that makes such a call convincing was in the repository.

There is a governance dimension the client took seriously. The material was outside the client's control entirely: no policy, no access review and no offboarding checklist would have found it, because it was not in the client's estate. The exposure was created by a third party's action after the relationship ended.

REMEDIATION DELIVERED

Contractor contacted directly; repository made private within twenty-four hours and subsequently deleted. Platform-side cache removal requested and confirmed.

Staging credentials in the scratch file rotated, notwithstanding that they were believed inactive.

Authentication design reviewed specifically against the documented bypass conditions, on the assumption that the material should be treated as known to an adversary.

Contractor offboarding process amended to include a documented handover and deletion attestation covering material held in personal accounts, and periodic code-hosting reconnaissance for client identifiers added to the monitoring scope.

OUTCOME

Both Critical findings were escalated on discovery rather than held for the report. All three undocumented hosts were offline the same day and every exposed secret was rotated within twenty-four hours. All four findings were fully resolved within seventy-two hours of report delivery.

The lead investor's technical due diligence proceeded on schedule and raised no security findings. The round closed on its original timetable at the agreed valuation. The client retained continuous external asset discovery and breach-corpus monitoring, which is the durable outcome — the four findings were closed, but the process gap that produced them was closed as well.

Value delivered

4h	72h	0	On time
from discovery to client notification	to full remediation of all findings	security findings raised in investor diligence	round closed at agreed valuation

SECTION 06 · THREAT ACTOR ATTRIBUTION

European engineering firm, repeat targeted intrusions

Three intrusions in fourteen months, each contained, none explained. The client could stop the incidents but could not answer why they kept happening.

Engagement profile

Client	Specialist engineering manufacturer, privately held
Sector and geography	Precision engineering · European Union, single primary site
Commercial context	Proprietary design portfolio representing the majority of enterprise value
Engagement driver	Three targeted intrusions in fourteen months, contained but unexplained
Scope	Attribution assessment, motive analysis, strategic recommendation
Duration	Six weeks, extended by four weeks to support legal proceedings
Prior work	Incident response and containment delivered by the client's MSSP

Situation

The client had been broken into three times in fourteen months. Each intrusion was detected and contained by a competent managed security provider. Each was focused specifically on proprietary design data rather than on customer records, finance systems or anything that could be monetised generically. Each evaded the detection tooling that had been strengthened after the previous one.

The MSSP had done its job. Its remit was detection and containment, and it delivered both. What it could not do — and was never contracted to do — was explain the pattern. Three targeted intrusions against a mid-market manufacturer, all aimed at the same category of data, is not opportunistic behaviour. The client was being selected.

The strategic problem was that the client was making defensive investment decisions without knowing what it was defending against. Board discussion had reached the point of considering whether to fragment the engineering function across jurisdictions — an expensive, disruptive change proposed in the absence of any understanding of the adversary. The engagement was commissioned to replace that vacuum with an assessment.

Findings summary

ID	FINDING	SEVERITY	IMPACT DOMAIN
TAA-01	All three intrusions linked to one another and to three prior campaigns by a shared infrastructure artefact	CRITICAL	Strategic · Legal · Investment
TAA-02	Targeting directive naming the client's product sector posted six weeks before the first intrusion	CRITICAL	Motive · Persistence of threat
TAA-03	Tradecraft concordance with seven prior campaigns across three jurisdictions	HIGH	Attribution confidence · Predictive
TAA-04	Motive assessed as commissioned competitive collection on behalf of a commercial end customer	HIGH	Strategic · Commercial

TAA-01

All three intrusions linked to each other and to three prior campaigns by a shared infrastructure artefact

CRITICAL Confidence: High · Source: Certificate transparency, passive DNS, host correlation · Corroborated against two commercial intelligence sets

EVIDENCE

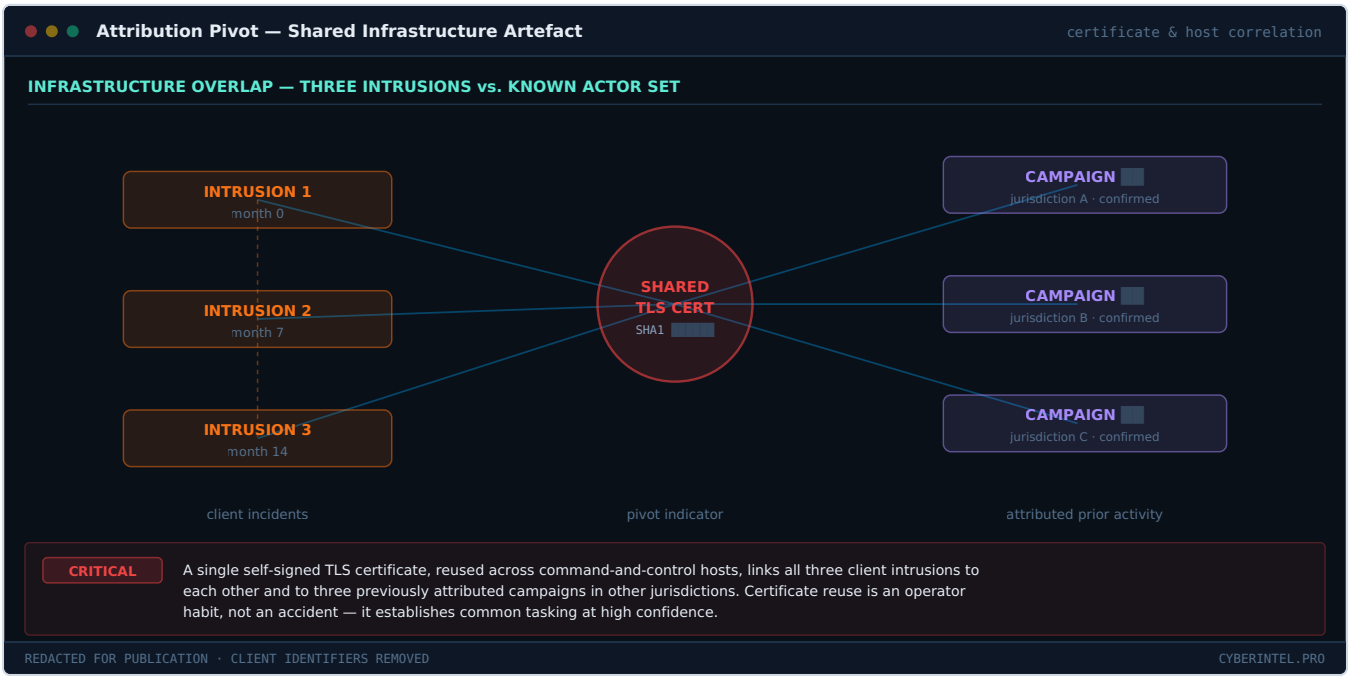

Exhibit TAA-01. A single self-signed TLS certificate reused across command-and-control infrastructure links all three client intrusions to each other and to three previously attributed campaigns in other jurisdictions.

ASSESSMENT

Command-and-control infrastructure recovered from all three incidents shared a single self-signed TLS certificate. The same certificate fingerprint appeared on hosts used in three previously attributed campaigns in three other European jurisdictions, spanning a period of roughly two years.

Certificate reuse is an operator habit rather than an accident. Infrastructure is routinely rotated between operations; the certificate is often generated once and carried forward because generating a new one is a step that produces no visible benefit. It is one of the more reliable pivots available precisely because it reflects working practice rather than intent.

Two commercial intelligence providers independently associated the certificate with the same actor set, which is the corroboration that lifts this from a lead to a finding. The alternative explanation — that a certificate leaked and was adopted by unrelated actors — was considered and does not fit: the campaigns also share tradecraft, sector focus and infrastructure-provisioning patterns, which a leaked certificate would not explain.

BUSINESS IMPACT

The strategic consequence is that the client stopped treating three incidents as three problems. A single actor with two years of demonstrated persistence, returning after each containment, is a fundamentally different proposition from a series of unrelated opportunists. It changes the defensive question from how to keep them out to what happens when they get in again.

That reframing had a direct and quantifiable effect on investment. The board had been considering fragmenting the engineering function across jurisdictions at substantial cost and operational disruption. The assessment established that the adversary was not exploiting a perimeter weakness that geography would fix; it was persistently targeting a specific data category through whatever route was available. The correct investment was in protecting the data, not in relocating the people, and the fragmentation proposal was withdrawn.

The finding also carried direct legal weight. Established linkage between the intrusions and prior attributed activity was the evidential foundation for the proceedings the client subsequently brought. Without it, the client had three unexplained incidents; with it, it had a documented pattern of conduct attributable to an identifiable actor set.

Finally, the finding is predictive. Knowing which actor set is responsible means knowing its historical tempo, its typical dwell time, its preferred initial access route and its behaviour after containment. Detection engineering could be tuned to a specific adversary rather than to a generic threat model.

REMEDIATION DELIVERED

Full indicator set derived from the certificate pivot — infrastructure, hosting patterns and provisioning behaviour — supplied to the MSSP for retrospective hunting and forward detection.

Retrospective search conducted across available telemetry for contact with the wider infrastructure set, establishing that the three known incidents were the full extent of successful access rather than assuming it.

Certificate and infrastructure monitoring established so that new hosts provisioned by the same operator generate an alert before an intrusion attempt rather than after.

TAA-02

Targeting directive naming the client's product sector posted six weeks before the first intrusion

CRITICAL Confidence: High · Source: Monitored closed forum, access held lawfully · Captured contemporaneously

EVIDENCE

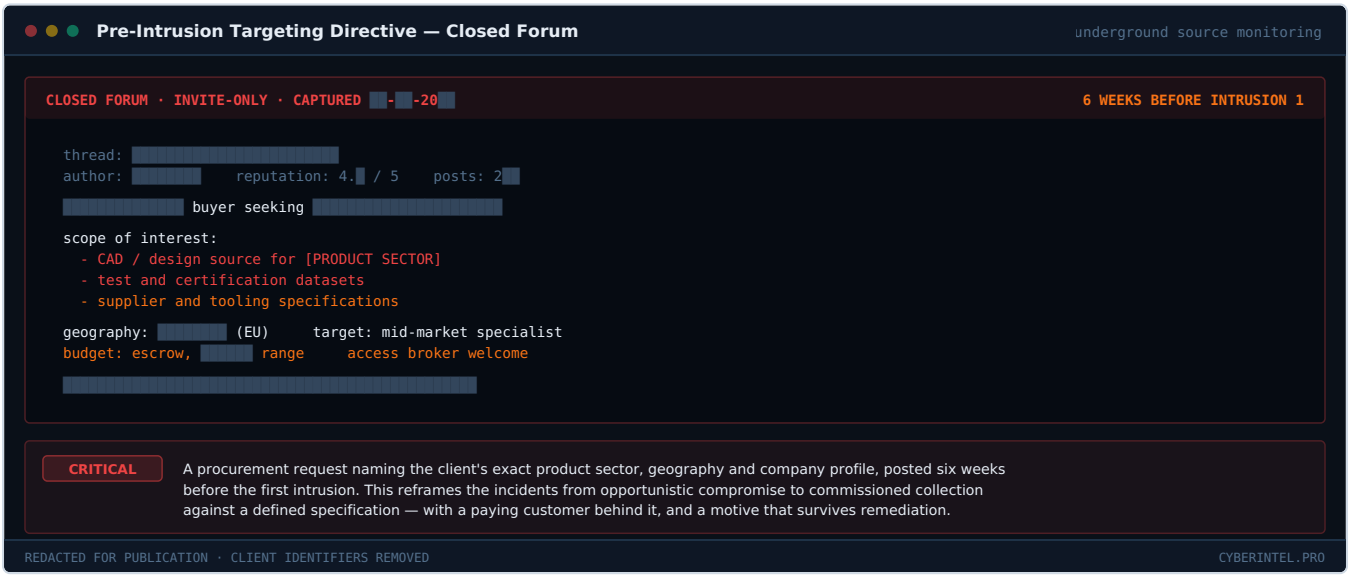

Exhibit TAA-02. Procurement request posted to an invite-only forum specifying the client's exact product sector, geography and company profile, six weeks before the first intrusion.

ASSESSMENT

A procurement request was posted to an invite-only forum six weeks before the first intrusion. It specified a product sector matching the client's speciality precisely, a geography matching the client's location, and a target profile matching the client's size and market position. It sought design source data, test and certification datasets, and supplier and tooling specifications.

The post offered escrowed payment and explicitly invited access brokers. It was captured contemporaneously through monitoring rather than reconstructed afterwards, which matters for its evidential value.

The specificity is what carries the assessment. Generic requests for industrial data are common. A request naming this sector, this geography and this company profile, within a jurisdiction where the client is one of a small number of firms meeting the description, is not plausibly coincidental. The requested data categories also correspond precisely to what was taken in the intrusions.

BUSINESS IMPACT

This finding reframed the entire matter for the client's board. Opportunistic compromise is a security problem: contain it, remediate, improve. Commissioned collection against a written specification, with a paying customer, is a commercial problem that security controls alone cannot resolve. The demand does not disappear when the intrusion is contained — it persists, and it will be met by a different route or a different contractor.

The finding also establishes that the threat survives remediation. A buyer who wants this data and is willing to pay for it will still want it after every technical control is improved. That understanding is what justified the shift in strategy from perimeter hardening to restructuring how the intellectual property was held and handled internally.

There is a supply-chain implication the client had not considered. If the sector is being shopped generically, the client's suppliers, certification partners and joint-venture counterparties are alternative routes to the same data — and they were outside the scope of every control the client had implemented.

For the legal proceedings, evidence of a commercial market for the specific data taken was material to establishing that the intrusions were commercially motivated rather than incidental, which bore directly on the remedies available.

REMEDIATION DELIVERED

Continuous monitoring established for the client's sector, product terminology and company identifiers across the relevant closed communities, providing forward warning rather than retrospective explanation.

Supplier and certification-partner exposure reviewed as an alternative route to the same data, extending the threat model beyond the client's own estate.

Board briefing delivered reframing the matter from an IT security issue to a commercial intelligence threat with a persistent demand side, which is what unlocked the strategic response.

TAA-03

Tradecraft concordance with seven prior campaigns across three jurisdictions

HIGH Confidence: High · Source: Incident artefacts compared against attributed campaign reporting

EVIDENCE

Tradecraft Concordance Matrix campaign comparison

TACTIC / TECHNIQUE OVERLAP — CLIENT INCIDENTS vs. SEVEN PRIOR CAMPAIGNS

TECHNIQUE	PRIOR CAMPAIGNS	C1	C2	C3	C4	C5	C6	C7	MATCH
Initial access — supplier-themed spear-phish		●	●	●	●	●	●	●	7/7
Signed but revoked driver for persistence		●	●	–	●	●	●	–	5/7
Living-off-the-land lateral movement (WMI)		●	●	●	●	●	●	●	7/7
Staging in engineering file-share only		●	●	●	–	●	●	●	6/7
Exfil via cloud-storage API, business hours		●	●	●	●	●	–	●	6/7
Anti-forensics: selective log truncation		●	–	●	●	–	●	●	5/7
Dwell before collection > 40 days		●	●	●	●	●	●	●	7/7
AGGREGATE TECHNIQUE CONCORDANCE									88%

HIGH Two techniques appear in all seven prior campaigns and in all three client incidents: supplier-themed initial access and extended dwell before collection. Combined with the shared certificate, tradecraft concordance supports the attribution at high confidence rather than circumstantial similarity.

REDACTED FOR PUBLICATION · CLIENT IDENTIFIERS REMOVED CYBERINTEL.PRO

Exhibit TAA-03. Technique-level comparison between the client incidents and seven prior attributed campaigns. Two techniques appear in all seven; aggregate concordance is eighty-eight per cent.

ASSESSMENT

Techniques recovered from the three client incidents were compared against seven previously attributed campaigns targeting the same engineering sector across three jurisdictions. Aggregate concordance was eighty-eight per cent across the technique set examined.

Two techniques appeared in all seven prior campaigns and in all three client incidents: supplier-themed spear-phishing for initial access, and extended dwell — more than forty days — before any collection activity. Both are behavioural signatures rather than tooling artefacts, which makes them more durable indicators; tooling changes between operations, working method does not.

The remaining concordance covered persistence via a signed but revoked driver, living-off-the-land lateral movement, staging confined to engineering file shares, exfiltration through a cloud storage API during business hours, and selective log truncation. The pattern describes an operator who is patient, disciplined about blending with normal activity, and specifically interested in engineering data rather than in whatever is available.

BUSINESS IMPACT

Tradecraft concordance is what converts the infrastructure finding from a strong lead into a defensible attribution. Shared infrastructure alone admits alternative explanations — reuse, resale, compromise of the operator. Shared infrastructure plus shared working method plus independent motive evidence does not. This finding is the reason the overall assessment was stated at high confidence and survived challenge in a legal setting.

It also produced immediately actionable defensive value. Knowing the actor waits more than forty days before collecting means detection engineering can be tuned for long-dwell, low-activity presence — the hardest thing to catch, and the thing the client's tooling had been consistently missing. Knowing initial access is supplier-themed means phishing simulation and supplier verification could be focused where the actor actually operates.

The finding carried a forward-looking implication the client acted on. Selective log truncation indicates an operator who anticipates forensic review. Log integrity — write-once retention, off-host aggregation — moved up the client's priority list on the basis that the existing evidential record could not be relied upon in a future incident.

REMEDIATION DELIVERED

Detection engineering reprioritised toward long-dwell, low-signal presence, with specific detection content developed for the documented techniques.

Supplier-themed phishing simulation implemented, replacing the generic programme that did not reflect how this actor operates.

Log integrity controls implemented — off-host aggregation with write-once retention — to preserve the evidential record against selective truncation.

TAA-04

Motive assessed as commissioned competitive collection on behalf of a commercial end customer

HIGH Confidence: Moderate to High · Source: Analytic synthesis across TAA-01 to TAA-03 and sector reporting

ASSESSMENT

Drawing the preceding findings together: an actor set with state adjacency in prior reporting, operating against a commercial target, collecting a data category with no intelligence value but substantial commercial value, following a procurement request that offered payment.

The assessment is that the collection was commissioned competitive intelligence on behalf of a commercial end customer, most plausibly a competitor or a state-linked industrial entity in a jurisdiction pursuing capability in the client's sector. Confidence is moderate to high — high on the commercial rather than intelligence character of the collection, moderate on the specific identity of the end customer, which the evidence does not establish.

The alternative explanation — collection for state intelligence purposes with commercial framing as cover — was considered and assessed as less likely. The data categories sought are specific to manufacturing capability rather than to strategic or dual-use assessment, and the procurement request's commercial structure, including escrow, is inconsistent with state tasking. This alternative is recorded because it cannot be excluded.

BUSINESS IMPACT

Motive determines the correct strategic response, and the client had been operating without it. Collection for resale or espionage-for-hire ends when the data is obtained. Collection on behalf of a competitor pursuing the same market persists as long as the commercial rationale persists — which is to say, indefinitely.

This is what justified restructuring how the design portfolio was held rather than continuing to invest in keeping intruders out. If the adversary will return indefinitely, the design objective changes: assume eventual access, and ensure that access does not yield usable data. Compartmentalisation, encryption at rest with segregated key management, and watermarking so that any future leak is traceable to its source.

The commercial-motive assessment was material to the legal strategy. Competitive collection on behalf of an identifiable commercial beneficiary opens avenues — trade secret misappropriation, unfair competition — that are unavailable against an anonymous actor. The assessment shaped what proceedings were viable.

The finding also had procurement consequences. The client reviewed its counterparty relationships in the relevant market with the assessment in view, and adjusted what design detail was shared at which stage of a commercial discussion.

REMEDIATION DELIVERED

Intellectual property handling restructured on an assume-breach basis: compartmentalisation of the design portfolio, encryption at rest with segregated key management, and watermarking to make any future leak traceable.

Design data sharing in commercial discussions staged so that full detail is disclosed only at contractual commitment rather than during evaluation.

Attribution assessment prepared to evidential standard and provided in support of legal proceedings, including documentation of methodology and source reliability.

OUTCOME

The attribution assessment was accepted as expert evidence in the legal proceedings the client subsequently brought. Intellectual property handling was restructured so that a future successful intrusion would not yield usable design data — compartmentalised storage, segregated key management, and watermarking sufficient to trace any leak to its source.

The board's proposal to fragment the engineering function across jurisdictions was withdrawn once the assessment established that geography was not the relevant variable, avoiding substantial cost and disruption for no defensive gain.

Legal action was filed. Intrusion attempts ceased within weeks of filing and had not resumed at the point of last contact, eighteen months later. The causal link is not claimed with certainty — the timing is consistent with the proceedings being the deterrent, but other explanations exist and the client was told so.

Value delivered

3
incidents resolved into one attributed actor

88%
tradecraft concordance established

Withdrawn
costly restructuring proposal, avoided

18mo
no further intrusion attempts

SECTION 07 · FINANCIAL-SECTOR INVESTIGATION

Private equity founder due diligence

A subject who had passed standard background checks twice. Three material findings, none of them in English.

Engagement profile

Client	Mid-market private equity firm
Transaction	Secondary transaction, significant position
Subject	Founder and continuing executive of the target company
Commercial context	Transaction in final documentation, signing scheduled
Engagement driver	Enhanced founder due diligence beyond standard background screening
Prior diligence	Standard background check passed; vetted by a prior investor three years earlier
Duration	Four weeks, delivered ahead of the signing date

Situation

The client was finalising a significant secondary transaction. The subject — founder and continuing executive of the target — had passed a standard background check commissioned for this transaction, and had been vetted by a different institutional investor three years earlier. Nothing in the file suggested a problem.

The engagement was commissioned as a matter of process rather than suspicion. The client's investment committee had adopted enhanced founder diligence for transactions above a threshold, following an unrelated experience elsewhere in the portfolio. There was no specific concern about this subject.

The investigation produced three findings, two of them Critical. All three were material to the transaction. All three had been missed by two prior diligence processes conducted by competent providers. The common factor was not negligence: it was that the decisive records existed in languages and jurisdictions that English-language screening does not reach.

Findings summary

ID	FINDING	SEVERITY	IMPACT DOMAIN
FSI-01	Undisclosed insolvency in a prior business registered under a name variant in another jurisdiction	CRITICAL	Warranties · Transaction terms

ID	FINDING	SEVERITY	IMPACT DOMAIN
FSI-02	Regulatory inquiry into a prior employer where the subject held a board seat, documented in Hebrew	CRITICAL	Disclosure · Regulatory · LP relations
FSI-03	Corporate proximity to a subsequently sanctioned individual through a shared nominee director	HIGH	Sanctions · Compliance · Reputational

FSI-01

Undisclosed insolvency in a prior business registered under a name variant in another jurisdiction

CRITICAL Confidence: High · Source: Corporate registry, certified extract and translation obtained

EVIDENCE

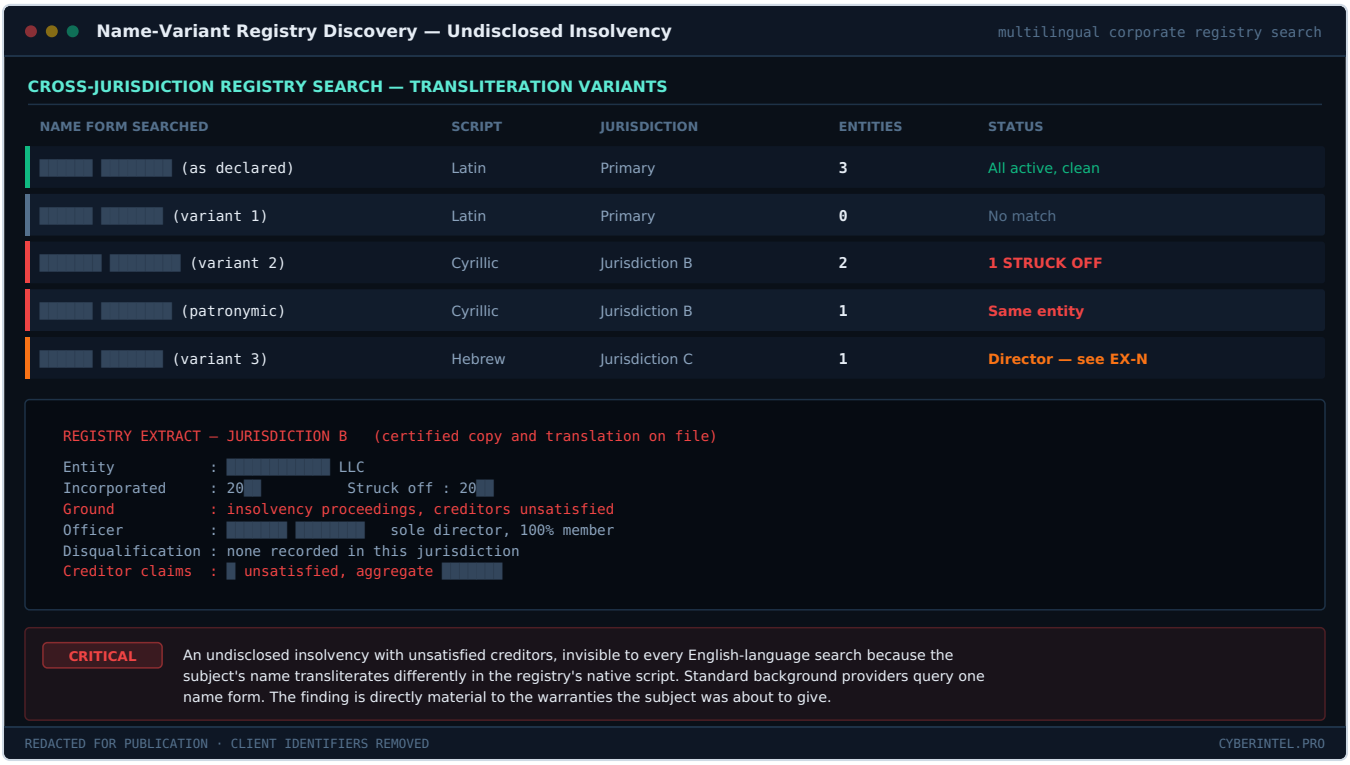

Exhibit FSI-01. Cross-jurisdiction registry search across transliteration variants of the subject's name. The Cyrillic variant returned an entity struck off following insolvency proceedings.

ASSESSMENT

Searching the subject's name in its declared Latin form returned three entities, all active and unremarkable. Searching systematic transliteration variants — Cyrillic forms, patronymic constructions, alternative Latin renderings — returned two further entities in a second jurisdiction under a Cyrillic variant of the same name.

One had been struck off following insolvency proceedings with creditor claims left unsatisfied. The subject was recorded as sole director and hundred-per-cent member. A certified registry extract and a certified translation were obtained; identity was confirmed through date of birth and a documented prior address, not through name similarity alone.

No disqualification was recorded, and none was applicable in that jurisdiction on these facts. The subject had not disclosed the entity in the transaction documentation. Whether the omission was deliberate could not be established from the record, and the report said so — the finding is that the fact exists and is material, not that it was concealed.

BUSINESS IMPACT

The finding is directly material to the warranties the subject was about to give. Transaction documentation of this kind routinely requires disclosure of prior directorships, insolvency events and unsatisfied creditor claims. An undisclosed insolvency with unsatisfied creditors would, on the client's own precedent documents, constitute a warranty breach discoverable after completion — which is the worst time to discover it, because the remedy is litigation rather than negotiation.

There is a character and judgment dimension the investment committee weighed separately from the legal one. A founder who has taken a business through insolvency is not thereby unsuitable; many strong operators have. A founder who does not disclose it when specifically asked raises a different question, and it is a question about what else has not been disclosed rather than about the insolvency itself.

The finding also exposed a systemic gap in the client's diligence process, which the client valued at least as highly as the finding. Two competent providers had searched one form of the subject's name. Any individual whose name transliterates across scripts — a substantial proportion of founders in the client's target markets — carries the same blind spot. The client changed its standing diligence specification as a result.

REMEDIATION DELIVERED

Certified registry extract and certified translation obtained and provided to the client's counsel as evidence rather than as assertion.

Identity confirmation documented through corroborating identifiers, so that the finding could withstand a challenge that the match was coincidental.

Full transliteration-variant search extended across all jurisdictions with a plausible connection to the subject, to establish whether further undisclosed entities existed. None were found, which is itself a useful finding for the client.

FSI-02

Regulatory inquiry into a prior employer where the subject held a board seat, documented only in Hebrew

CRITICAL Confidence: High · Source: Financial regulator enforcement bulletin, Hebrew-language publication

EVIDENCE

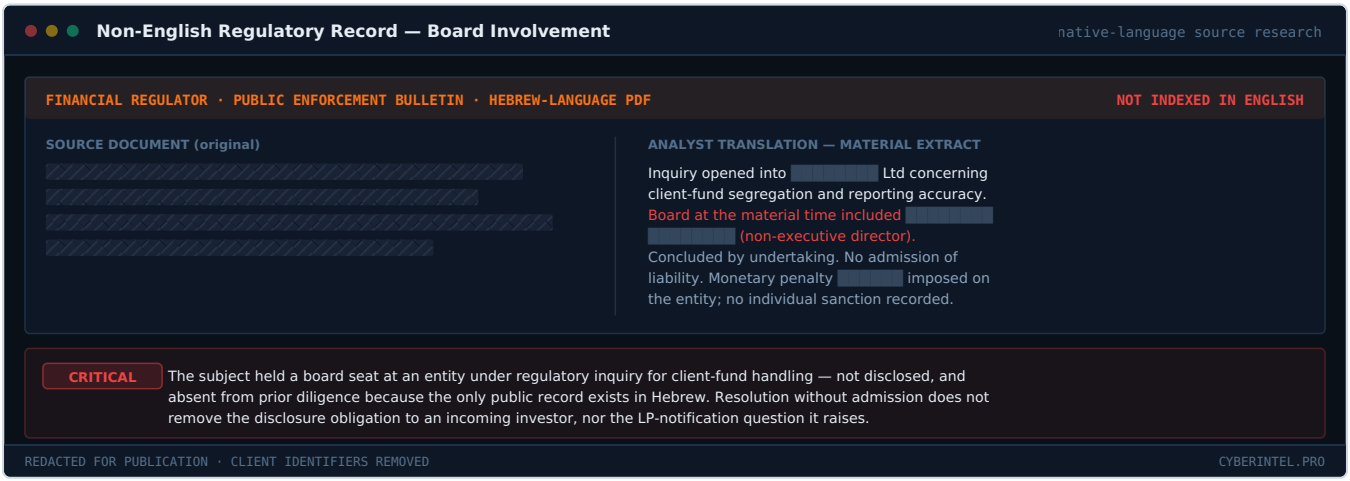

Exhibit FSI-02. Financial regulator enforcement bulletin published in Hebrew and not indexed in English. The subject is named as a non-executive director at the material time.

ASSESSMENT

A financial regulator in a third jurisdiction had opened an inquiry into an entity concerning client-fund segregation and reporting accuracy. The subject was named in the published enforcement bulletin as a non-executive director at the material time.

The matter concluded by undertaking. No admission of liability was made. A monetary penalty was imposed on the entity; no individual sanction was recorded against the subject or any other director.

The bulletin was published in Hebrew and was not indexed in English. It was not present in any commercial adverse-media or regulatory-screening database checked during the engagement. It was found by searching the regulator's own publications directly, in the local language — which is a matter of method rather than of luck.

BUSINESS IMPACT

Resolution without admission does not remove the disclosure obligation. Transaction documentation typically requires disclosure of regulatory investigations involving entities where the subject held office, regardless of outcome. Client-fund segregation is a particularly sensitive subject matter for an investor in the financial sector, because it goes to the governance of client money — the thing that a fund's own limited partners care most about.

The client's own LP obligations were engaged, and this drove the client's response more than the transaction terms did. Institutional limited partners commonly require notification of regulatory matters involving portfolio company principals. Discovering such a matter after completion, from a third party, would raise a question about the client's diligence rather than about the subject — and reputational damage to the manager is harder to repair than a bad deal.

The non-executive character of the role was assessed as mitigating but not eliminating. A non-executive director is not expected to have operational knowledge of fund segregation practice. A non-executive director is expected to disclose that the board they sat on was subject to a regulatory inquiry into it.

As with FSI-01, the systemic point was material. Regulatory publications in non-English jurisdictions are routinely absent from commercial screening databases. Any subject with a career history spanning such a jurisdiction carries this exposure, and the client had no process that would have caught it.

REMEDIATION DELIVERED

Source document, certified translation and a documented provenance chain provided to the client's counsel to support a specific disclosure request to the subject.

Scope of the subject's role, the period of tenure and the terms of resolution documented so that the investment committee could weigh the matter proportionately rather than react to a headline.

Native-language regulatory searching added to the client's standing diligence specification for all jurisdictions in a subject's career history.

FSI-03

Corporate proximity to a subsequently sanctioned individual through a shared nominee director

HIGH Confidence: High on the structure, no assessment offered on knowledge or intent

EVIDENCE

Exhibit FSI-03. Officer-level graph showing the subject and a subsequently sanctioned individual connected through a shared nominee director in a jurisdiction with no beneficial-ownership register.

ASSESSMENT

Officer-level analysis identified an individual who served as director of an entity in which the subject held an interest, and concurrently as director of a separate entity associated with a person subsequently placed under international sanctions. The shared officer displayed the characteristics of a professional nominee: directorships across a large number of unrelated entities, all in a single low-disclosure jurisdiction.

There is no direct relationship between the subject and the sanctioned individual in any record examined. The connection is two degrees, through the nominee. The sanctions designation post-dates the subject's involvement.

The finding is deliberately framed as structural proximity, not as an allegation. No assessment is offered as to whether the subject knew of the sanctioned individual, and nothing in the evidence suggests it. The jurisdiction has no public beneficial-ownership register, which means the ultimate ownership behind either entity could not be established in either direction — a limitation stated rather than papered over.

BUSINESS IMPACT

For a regulated investor, sanctions proximity is a compliance matter independent of intent. Enhanced due diligence obligations, and in some institutions escalation to a financial crime committee, are triggered by the structural fact rather than by any finding of knowledge. The client needed to know before signing because the obligation attaches on acquisition of the interest, and discharging it afterwards is materially more difficult.

The reputational asymmetry drove the client's response. A two-degree connection through a nominee director is, in substance, weak and probably meaningless. Reported by a journalist or raised by an LP, it does not read as weak — it reads as a private equity firm connected to a sanctioned individual, and the correction never travels as far as the claim. The value of finding it in diligence is the ability to document the analysis in advance rather than construct it under pressure.

The nominee structure carried its own signal, independent of the sanctions connection. Reliance on professional nominees in a jurisdiction with no ownership transparency is a legitimate arrangement and a common one. It is also a structure that limits what any investor can establish about who ultimately stands behind a counterparty, and the client factored that opacity into its view of the subject's broader arrangements.

Weighed in isolation this finding would not have affected the transaction. Weighed alongside two undisclosed matters, it contributed to a pattern the investment committee took into account — that the subject's affairs were more complex, and less fully disclosed, than the file suggested.

REMEDIATION DELIVERED

Full officer-level graph documented with source citations for each edge, allowing the client's compliance function to review the underlying records rather than the conclusion.

Enhanced due diligence file prepared in a form suitable for the client's financial crime committee and for retention as evidence of the analysis performed.

Sanctions and adverse-media monitoring established on the relevant entities and individuals for the holding period, so that a future designation is detected promptly.

OUTCOME

The transaction proceeded, but not on the original terms. It was restructured with enhanced representations and warranties addressing the specific matters identified, an extended indemnity period, and a portion of consideration placed in escrow against warranty claims. The subject provided explanations for both undisclosed matters which the investment committee accepted as adequate in substance while regarding the non-disclosure as relevant to how the relationship would be managed.

The deal closed on the revised terms. All three findings would have been missed by standard English-language due diligence — as they had been, twice, by two competent providers. The client amended its standing diligence specification to require transliteration-variant registry searching and native-language regulatory searching across every jurisdiction in a subject's history, which is the outcome with the longest tail.

Value delivered

3
material findings after two clean checks

3
languages and jurisdictions searched

Restructured
terms revised before signing

Pre-signing
delivered ahead of the deadline

SECTION 08

Cross-engagement analysis

Four engagements with different clients, sectors and objectives. The patterns that recur across all of them are more instructive than any individual finding.

Where the findings actually came from

Not one of the sixteen findings in this document required exploiting a technical vulnerability. Not one involved unauthorised access to a system. The severity distribution is heavily weighted toward Critical — nine of sixteen — and yet the collection methods were, without exception, passive.

This is the single most useful observation for a reader deciding whether an assessment of this kind is worth commissioning. The findings that mattered were not hidden behind defences. They were in registries, broker databases, breach corpora, certificate logs, DNS records, code-hosting platforms and public regulatory bulletins. What made them hard to find was not that they were protected, but that nobody had been asked to look in those places for that client.

FINDING ORIGIN BY CATEGORY

ORIGIN	FINDINGS	SHARE	HIGHEST SEVERITY
Assets the client did not know existed	4	25%	Critical
Records outside the client's own estate	5	31%	Critical
Non-English or non-Latin-script sources	3	19%	Critical
Aggregation of individually harmless public data	3	19%	Critical
Third-party action after a relationship ended	1	6%	High

Three patterns that recurred

01 **Competence was never the problem.** Every client in this document had done sensible things. A security engineer, an MSSP, a password manager, two prior background checks. In each case the controls worked correctly within their scope, and the finding sat outside it. The useful question for a reader is not whether their controls are good, but what those controls were scoped never to see.

02 **The decisive evidence was usually somewhere else.** In three of four engagements the material finding existed outside the client's estate entirely: a broker's database, a former contractor's personal repository, a foreign regulator's Hebrew-language bulletin, a nominee director's filing history. No amount of internal rigour reaches these, because they are not internal.

03 **Commercial consequence tracked position, not sophistication.** The exposures that produced the largest potential losses were among the least sophisticated. A forgotten development server is a trivial finding that happened to hold the production signing key. A DNS record nobody withdrew is a

housekeeping item that happened to be a credential-harvesting page on the client's own domain. Severity followed what the exposure touched, not how clever it was.

Timing and its effect on value

All four engagements were commissioned before an event rather than after one: a listing, a funding round, a legal filing, a signing. This is not a coincidence of the sample — it is the condition under which this work is worth most.

The same findings delivered after the event would have been considerably less valuable and considerably more expensive to act on. An undisclosed insolvency found before signing is a negotiating position; found afterwards it is a warranty claim. A production key found before investor diligence is a remediation task; found during diligence it is a valuation question. An impersonation account found before a listing is a takedown; found after a fraudulent approach it is an incident.

TIME FROM ENGAGEMENT START TO FIRST CRITICAL FINDING

ENGAGEMENT	FIRST CRITICAL FINDING	METHOD	CLIENT NOTIFIED
01 · Executive exposure	**Day 2**	Broker aggregation sweep	In report
02 · Attack surface	**Day 1**	Passive host enumeration	Within 4 hours
03 · Attribution	**Week 2**	Certificate transparency pivot	In interim briefing
04 · Financial investigation	**Day 6**	Transliteration-variant registry search	In report

In two of the four engagements, a Critical finding was established within forty-eight hours of starting. This is worth stating plainly because it cuts both ways: it demonstrates that the work does not require months, and it means the same exposures were available at the same cost to anyone else who thought to look.

SECTION 09

Recommendations

Drawn from what recurred across these four engagements rather than from general practice. Each corresponds to a specific finding above.

---

01 **Reconcile the asset inventory against what the internet can see, continuously.** EAS-01 existed because three hosts were live and not in the inventory. An inventory describes intent; external discovery describes reality. The gap between them is where the Critical findings live, and it can only be found by looking from the outside in.

02 **Treat a leaked password as a leaked method, not a leaked string.** EDE-02 mattered because two breaches revealed a construction rule that survived every rotation. Rotating the exposed password addresses the instance. Identifying and replacing every hand-made password addresses the class.

03 **Search names in every script and variant a subject plausibly uses.** FSI-01 was invisible to two competent providers because they searched one name form. For any subject with a cross-script name history, single-form searching is not diligence — it is the appearance of diligence.

04 **Search regulators directly, in the local language.** FSI-02 was absent from every commercial screening database checked. Adverse-media aggregators index what is indexed. Primary sources in the local language are the only reliable route to non-English regulatory records.

05 **Tie DNS record lifecycle to vendor offboarding.** EAS-03 persisted for two years after the vendor relationship ended because nothing connected contract termination to a DNS review. Make the offboarding checklist include the delegation, and the class of finding disappears.

06 **Extend executive protection to the household.** EDE-04 came entirely from family members' public accounts, not the subject's. An executive's own discipline is necessary and not sufficient. Brief the household, explain aggregation, and audit tagging permissions.

07 **Assume material held by former contractors still exists.** EAS-04 sat in a personal repository outside all client governance for fourteen months. Offboarding should include a deletion attestation, and periodic reconnaissance for client identifiers on code-hosting platforms should be routine.

08 **Establish motive before choosing a defensive strategy.** TAA-04 prevented an expensive restructuring that would have addressed the wrong variable. Where intrusions repeat, understanding why determines whether to invest in keeping an adversary out or in ensuring that getting in yields nothing usable.

SECTION 10

Scope, limitations and disclaimer

What this document is, what it is not, and what qualifies the assessments it contains.

Anonymisation

Every client and subject detail in this document has been removed or altered. Company names, individual names, domains, addresses, dates, financial figures, jurisdictions where identifying, and sector descriptions have been generalised or replaced. Where a specific figure appears — a count of exposed credentials, a percentage, a duration — it reflects the actual engagement.

Evidence exhibits are reconstructions that reproduce the structure, content type and analytical substance of the original material with all identifying values redacted. They are not screenshots of client deliverables and are not represented as such. They are included because the structure of the evidence is what makes a finding comprehensible.

The four engagements are real and were completed for real clients between 2023 and 2025. This document is published with the informed consent of the clients concerned, each of whom reviewed and approved the anonymised account of their engagement before publication.

Limitations inherent to the work

Open-source intelligence establishes what is discoverable at a point in time. Absence of a finding is not evidence of absence: it means that the sources examined, within the agreed scope and period, did not contain it. This is stated in every engagement and is repeated here because it is the most commonly misread aspect of this work.

No engagement in this document involved access to any system, account or network without authorisation. Where a finding required confirming that a service was live, verification was limited to unauthenticated interaction with a public endpoint. Assessments that a recovered credential is likely to be current are inferences from format and reuse patterns, never from an authentication attempt.

Attribution assessments express analytic judgment, not legal or forensic proof. The assessment in Engagement 03 is stated at high confidence with its reasoning and its alternative explanation on the record. It was accepted as expert evidence in one proceeding; that acceptance is a fact about that proceeding and is not a general warranty.

Outcomes described are those reported by clients or directly observed. Where a causal link between the work and an outcome is asserted, it is asserted only where the connection is direct. Where timing is suggestive but causation is not established — as with the cessation of intrusion attempts in Engagement 03 — that is stated.

Status of this document

This document is provided for information. It is not advice, and it does not create a professional relationship of any kind. It is not a representation that comparable findings or outcomes would be produced in any other engagement; every engagement depends on its own facts, scope and circumstances.

Nothing here should be read as an allegation against any identified or identifiable person or entity. Where an assessment concerns a third party — a threat actor set, a nominee director, a sanctioned individual — it is stated at the confidence level the evidence supports, with alternative explanations recorded where they exist.

ENGAGEMENT ENQUIRIES

Engagements are delivered personally by Karen Shahbazian or under direct supervision. Initial scoping discussions are without charge and without obligation.

Email	**contact@cyberintel.pro**
Web	**cyberintel.pro**
Free scoping call	**20 minutes, no obligation**
Paid initial assessment	**60-minute confidential consultation**