/ INSIDER THREAT & EMPLOYEE DATA THEFT 01A · TRIAGE

Insider Threat Triage Consult

€100 · One-off · secure checkout

> A 90-minute scoping call: what's suspected, which evidence sources exist, whether there's legal basis to investigate — and a fixed quote for the full case.

// DELIVERABLES

- A 90-minute scoping call with a forensic examiner.
- Confirmation of which evidence sources exist and are still recoverable — devices, email, cloud, logs.
- An assessment of whether there is a legal basis to investigate.
- A fixed, written quote for the full Employee Data Theft Investigation.
- Immediate evidence-preservation guidance to avoid spoliation before the call.

// EXPECTED OUTCOMES

- You know whether a defensible case can be built before committing budget.
- Volatile or time-limited evidence is preserved rather than lost.
- A clear go / no-go decision with a fixed price for the next phase.

// TIMELINE

90 minutes, scheduled on booking. Intake 24 / 7 / 365, response target under one hour.

// METHOD OF ENGAGEMENT

Every case follows the same backbone, scoped to the matter.

PHASE_01 Triage · scoping
Confirm what's suspected, which evidence sources exist, the legal basis, and a fixed quote.

PHASE_02 Forensic acquisition
Bit-for-bit imaging of devices, mailboxes and logs — hashed (SHA-256), write-blocked. Chain of custody opens here.

PHASE_03 Analysis · reconstruction
Reconstruct what happened and when — separating what the evidence proves from what it merely suggests.

PHASE_04 Reporting · findings
A plain-language account for decision-makers plus an exhibit-referenced technical annex built to survive scrutiny.

PHASE_05 Testimony · referral
As needed: regulator packaging, law-enforcement referral, expert statements and courtroom testimony.

INSIDER TRIAGE SECURE CHECKOUT