/ INSIDER THREAT & EMPLOYEE DATA THEFT 01B · INVESTIGATION

Employee Data Theft Investigation

from €1,500 · Quote range · scoped

> Forensic review of an employee's devices, email and cloud access to establish data or intellectual-property theft, with a defensible evidence trail.

// DELIVERABLES

- Forensic review of the employee's devices, email and cloud access.
- A defensible evidence trail: what data or IP left, when, and by whose hand.
- Bit-for-bit, hash-verified acquisition of each in-scope exhibit.
- An exfiltration finding with record counts and destinations where the evidence supports them.
- A written report — plain-language summary plus an exhibit-referenced technical annex.

// EXPECTED OUTCOMES

- A clear, evidence-backed answer to whether data or IP was taken.
- Findings packaged to support HR, civil, or regulatory action.
- An unbroken chain of custody from acquisition to report.

// TIMELINE

Acquisition within 24–48 h of instruction; analysis typically 1–3 weeks; reporting ~1 week. Exact timeline scoped at triage.

// 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 | INVESTIGATION | COURT-READY