/ MALWARE, RAT & MAAS EXFILTRATION

05B · INVESTIGATION

Exfiltration Investigation — Endpoint

from €850 · Per device · quote

> Full analysis of a malware-infected laptop, desktop or server, including the exfiltration timeline and data-loss scope.

// DELIVERABLES

- Full forensic analysis of a malware-infected laptop, desktop or server.
- An exfiltration timeline and data-loss scope.
- Confirmation of the infection and reconstruction of what left the device.
- An assessment of exactly what data was exposed, within the evidence.

// EXPECTED OUTCOMES

- A definitive answer on what got in and what left.
- A data-exposure scope to inform breach and notification decisions.

// TIMELINE

Per-device engagement; acquisition within 24–48 h, analysis and reporting scoped at kickoff.

// 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.

MALWARE | ENDPOINT | PER DEVICE