DISCRETION BY DESIGN · CLIENT EYES ONLY · PRINTABLE EXECUTIVE SUMMARY

The Mirror · Executive Summary

Engagement PI-M-2026-0387 · Subject M.V. · Delivered 12 May 2026

OVERALL EXPOSURE — HIGH

Across seven investigation categories, the subject's footprint sits in the **moderate-to-high** band for a German professional at partner level. The public-facing surface — LinkedIn, the firm directory — is well-managed. Exposure concentrates in three areas the subject is unlikely to have looked at recently.

01	Forgotten accounts on platforms the subject no longer uses, still publicly indexed.	MEDIUM
02	Old emails appearing in four documented public breaches (2012–2019), at least one credential pair still circulating.	HIGH
03	Two German people-search platforms surface assembled biographical data — name, city, age, two relatives.	HIGH

Headline counts

Categories examined	7
Distinct findings recorded	23
High-severity findings	6
Confirmed breaches with credential exposure	4
People-search platforms surfacing the subject	5
Recommended immediate actions (within 7 days)	4

What this means in practice

A motivated researcher — a journalist, a competitor's due-diligence team, a social engineer building a spear-phishing pretext — could in under two hours assemble: the subject's current employer and seniority; one current home city; an age band; the names of at least two family members; a personal email address; and a credential pair that has appeared in at least one large credential-stuffing list. None of this required dark web access. All of it was reachable from public sources.

The full report contains the 23 detailed findings, the per-category investigation, the risk synthesis, and the prioritised action plan covering immediate, short-term, and long-term measures.