/ OFFENSIVE

Mock Ransomware Attack

€2,500
ONE-OFF

Simulated ransomware exercise to expose gaps in detection, response and recovery — before the real thing does.

// DELIVERABLES

- A simulation plan and rules of engagement agreed up front.
- Reconnaissance followed by a focused, customised attack plan against key individuals.
- A controlled, non-destructive simulation of ransomware against an agreed scope, mapped to known attacker techniques (MITRE ATT&CK).
- A detection-and-response gap report.
- An assessment of backup and recovery capability, with prioritised recommendations.

// EXPECTED OUTCOMES

- Evidence of whether detection, response and recovery actually work under pressure.
- A prioritised list of the gaps that matter most.
- Readiness evidence for leadership, insurers and auditors.

// METHOD OF ENGAGEMENT

A controlled, non-destructive exercise run remotely — combining a technical simulation of ransomware techniques with observation of the response process and a recovery test.

// TIMELINE

Indicative: ~2–4 weeks covering planning, execution and reporting.

- Project management is included in all prices.