DEEP INFOSEC / 90-DAY PROGRAMME

Reduce the risk that matters to your business within 90 days

You have security tools, teams and remediation backlogs. The difficult part is deciding which combination of issues threatens a critical service, what must change first, and how to demonstrate that the change worked. Our Risk Compression Sprint brings those decisions into one time-bound engagement. Deep InfoSec works with your security, cloud, identity and business-service owners; Deep Advisor supplies the attack-path analysis and scenario evidence.

30 / 60 / 90

Days 1–30 · Understand the real exposure

We agree the critical services in scope, connect authorized scanner, cloud and identity evidence, map dependencies and establish a reproducible risk baseline. We distinguish an isolated issue from a viable route to business impact.

Days 31–60 · Remove the most consequential paths

Your owners review the proposed remediations with our architects. We test mitigations, change identity and network controls where authorized, and prioritize work that breaks multiple attack paths rather than merely changes a severity score.

Days 61–90 · Prove the reduction and transfer ownership

We retest the paths affected by remediation, document the evidence, prepare a board-level decision record and hand over an ordered workstream for controls that remain.

Included in the first 90-day scope

- One named critical business service and its documented owner
- Up to three authorized evidence sources (for example scanner, cloud security and identity)
- One agreed architecture/identity perimeter and up to five priority attack-path hypotheses
- One remediating workstream selected with the service owner, plus retesting and a board-ready handover

Team and decision responsibilities

- Deep InfoSec: programme lead, security architect, attack-path analyst and remediation/verification engineering as scoped
- Your organization: service owner, technical access, source exports or connectors, change-window approval and acceptance signatory

- Third parties: platform or field changes requiring their authority are scheduled and approved by the responsible operator

Indicative 90-day programme budget

€24,000–€58,000, excluding applicable tax · 25–45 consulting days across the 90-day period

Acceptance and handover

- Day 30: signed scope, asset/dependency map, evidence-source register and baseline risk paths
- Day 60: change decisions, responsible owners and implementation/compensating-control records
- Day 90: retested paths, residual-risk register, operating handover and management decision brief

You receive a critical-service dependency map, prioritized attack-path register, risk/impact/recovery view, remediation decision log, tested control changes and a 90-day executive report. Your team provides technical access, service ownership and change approval; Deep InfoSec provides analysis, engineering, verification and the handover pack.

The programme begins with one bounded service or portfolio and can be extended into ongoing Deep Advisor monitoring or a managed engineering service.