DEEP INFOSEC / ENGINEERING ACCOUNT

From finding overload to a defensible remediation plan

Your scanners, cloud controls, application tests and identity reviews do not all measure the same thing. A long list can therefore obscure a short and dangerous sequence: an externally reachable service, a privileged identity, and an unsegmented business application.

We collect the relevant outputs, normalize duplicate records and trace reachability, privilege and business-service dependency. Deep Advisor can generate plausible attack paths that existing rule sets have not described, evaluate their prerequisites, and link each path to potential mitigations. Analysts review the evidence and challenge alternate paths before recommending a change.

Critical services before scanner counts

The starting question was which assets carried the service, where access originated and who could authorize a fix. Scanner findings were associated with application owners, reachable network segments, identities and the relevant business process. The resulting map made it possible to distinguish a technical defect from a path that could reach something important.

Findings became linked paths

Duplicate records, outdated components and control alerts were reconciled to their underlying systems. Analysts then examined entry points, service identities, lateral reachability and the controls that interrupted or enabled each path. Deep Advisor evaluation used those relationships to identify plausible sequences and attach candidate mitigations to the affected steps.

One decision can close several exposures

A change to network reachability or a privileged identity can interrupt more than one path. The service owner compared those changes with patching, compensating controls and maintenance constraints. The outcome was an ordered engineering plan with responsibility, prerequisites and a check for unintended operational effects.

4,000 findings to 14 outstanding

In a documented senior-practitioner vulnerability-remediation engagement, the operational register moved from approximately 4,000 findings to 14 remaining items at the recorded checkpoint. The result reflects a managed programme of analysis, owner assignment, corrective work and verification. The before/after register must accompany any buyer-specific request for supporting evidence.

Evidence the next team can use

The handover connects each high-priority path to its affected service, initial evidence, chosen intervention, accountable owner, implementation record, retest and residual work. Leadership receives a decision summary; engineering teams retain the technical register and reproducible checks.

Acceptance and handover

The team receives a path register, before-and-after exposure views, ownership of each remediation, acceptance tests and a management explanation of what changed. A documented vulnerability-remediation engagement reduced an operational backlog from 4,000 findings to 14 outstanding items.

For a scoped assessment contact sales.advisor@deepinfosec.com.