DEEP INFOSEC / PUBLIC EVALUATION

Deep Advisor: turn disconnected findings into a defensible remediation decision

Evaluate attack-path context, evidence, control ownership and how priorities change after a corrective action.

Work with the information already available

The starting point is not a replacement scanner. Your security team selects representative findings from vulnerability management, cloud configuration, IAM, source control and detection systems. The evaluation determines which identities, assets, privileges and business services can be related and which remain outside the model. Data sources are agreed case by case; a category of integration should never be confused with a certified connector.

Show why the sequence matters

An exposed administrative service, an overprivileged account and a weak segmentation rule may sit in three different queues. Deep Advisor explores whether they form a connected path toward a critical service. For each asserted relationship, the evaluator should be able to inspect the relevant evidence, assumptions and uncertainty. Owners can compare the effect of removing a privilege, changing a route or restricting an endpoint.

Carry the decision through to closure

The accepted output is more than a risk heatmap. Each actionable path links business impact, technical evidence, a proposed intervention, the accountable owner, retest conditions and an explanation suitable for a CISO or regulator. The pilot includes deliberate false associations and incomplete data so that the limits of the model are visible in the decision record.

How an evaluation works

1. Select a representative service — Agree the business service, asset inventory, sample findings and access boundaries.

2. Build and challenge sample paths — A technical reviewer challenges every link and examines missing evidence and benign explanations.

3. Exercise remediation alternatives — Compare control changes, operational costs, path disruption and evidence needed for closure.

4. Review the decision record — Evaluate reproducibility, analyst effort and the usefulness of executive and engineering outputs.

What your team receives

The evaluation produces a source-and-identity map, validated path examples, a prioritised remediation register, model-assumption notes, sample executive decisions and a retest protocol.

Send a procurement-ready request

I want to evaluate Deep Advisor against [critical service] using [scanner/cloud/IAM/EDR categories]. The team has [approximate finding volume] and needs to decide [specific remediation question]. Please propose data boundaries, evaluation outputs, technical reviewers and a priced pilot.

sales.advisor@deepinfosec.com