Deception Technology: What it is, why it works, and how to trap attackers early

Gridinsoft Help Center

What it is

Why it works

Attackers look for quiet, easy wins. Decoys behave like real assets (logins, data, services), so any touch is suspicious by design-lighting up detections without drowning you in noise.

How it works

- Deploy decoys: faux databases, endpoints, shares, and cloud assets.
- Seed breadcrumbs: tempting creds/paths that only lead to traps.
- Detect & learn: capture IOCs, commands, and movement for faster response.

Where to use it

- High-risk segments (finance, HR, domain admins)
- Lateral movement paths in AD/cloud
- Remote access gateways, VPNs, and jump hosts

Quick start

- Map likely attacker paths.
- Drop a few high-quality decoys and unique honey-creds.
- Wire alerts to IR playbooks; isolate on first touch.
- Rotate decoys regularly and mine findings for hunt rules.