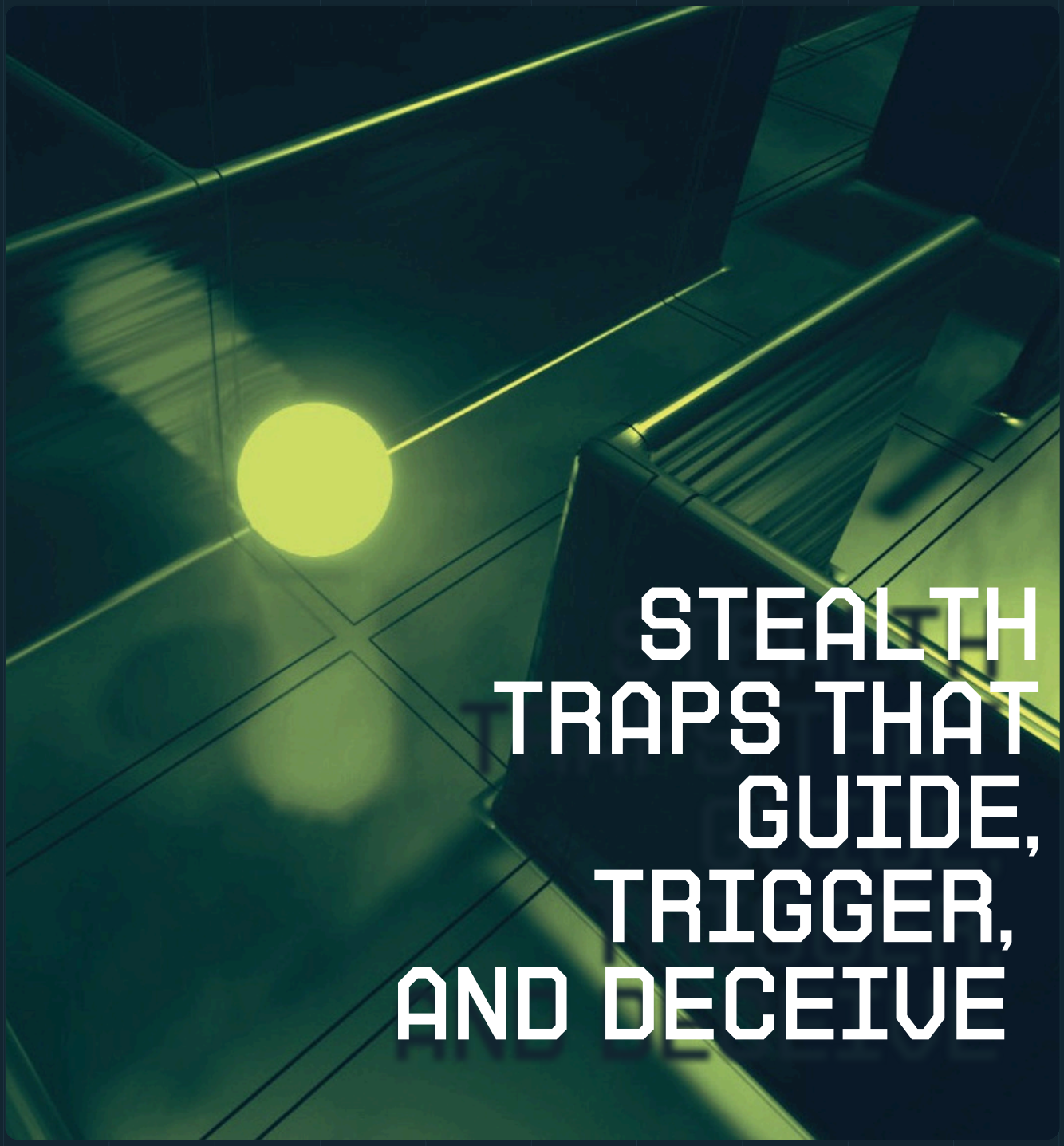
CYBERTRAP

ARTIFACT MANAGER

Engagement Layer



Artifact Manager deploys realistic digital assets—such as fake credentials, mapped drives, and decoy access links—across endpoints and cloud workloads to silently attract intruders and steer them into deception zones.

CYBERTRAP

Engagement Layer

ARTIFACT MANAGER

As the first point of contact in CyberTrap's deception framework, Artifact Manager plants stealth traps across your environment that adversaries instinctively interact with. These artifacts are crafted to appear legitimate within your infrastructure and are contextually placed to provoke curiosity, misuse, or movement, without alerting the attacker to their synthetic nature.

The system utilizes a multi-layered approach:

- Lures are enticing bait: files, tokens, or links, that trigger interest and initiate engagement.
- Breadcrumbs are navigational hints, such as registry entries or cached credentials, that lead attackers toward controlled decoy environments.
- Honey tokens act as precision tripwires, triggering immediate, silent alerts upon access or exfiltration attempts.

Artifact placement is driven by AI-based reconnaissance analysis and tailored to attacker tactics, ensuring that each asset serves a tactical purpose in shaping adversary behavior. Whether embedded in endpoint file systems, cloud repositories, or identity directories, these stealth elements function as an invisible early warning grid-detecting intent and enabling proactive containment.

USER BENEFITS:

- Early-stage detection through strategically placed artifacts
- Guided adversary movement via realistic breadcrumbs
- Covers both cloud and endpoint infrastructure seamlessly
- Operates invisibly without affecting production performance

Let's talk

contact@cybertrap.com +43 1 890 4700 cybertrap.com