Cyber deception

Turn any adversary contact into an unambiguous alarm

Cyber deception places decoy systems and planted lures on the kit that no legitimate user has any reason to touch. Because the bait exists only to be tripped, a single interaction with it is high-confidence evidence of an intruder, with far less noise than signature-based alerting.

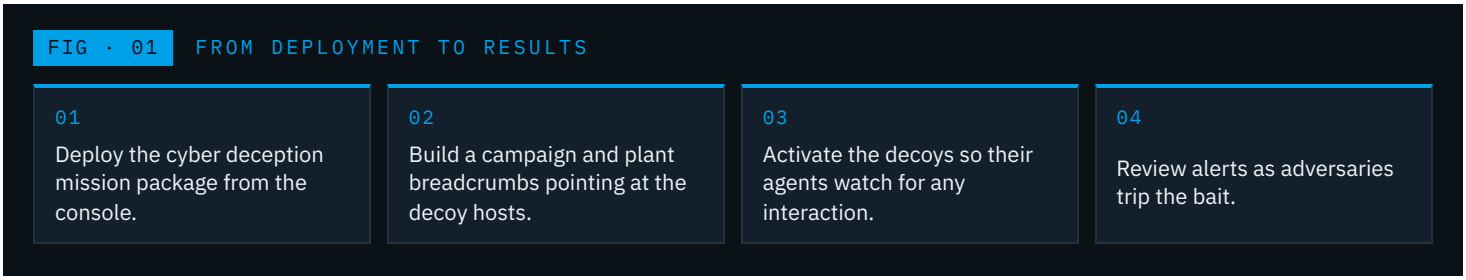
01 · WHY IT MATTERS

- A decoy has no legitimate use, so any contact with it is an incident by definition.
- Deception catches the quiet credential-abuse and lateral-movement moves that evade signature tools.
- Alerts carry context about what the adversary touched, not just a rule name.

02 · HOW IT WORKS ON RHOMBUS

- The console deploys the deception control plane and decoy hosts as a mission package.
- Campaigns pair decoys with breadcrumbs, such as fake credential files, shell history and planted keys, to lure the adversary.
- A hidden host agent watches each decoy and reports interactions through a relay to the deception control plane.
- Alerts forward to the kit's threat-intelligence store, team chat and network security monitoring.

FIG · 01 FROM DEPLOYMENT TO RESULTS



03 · DEFENSE & GOVERNMENT

- Defensive cyber operations gain early, high-confidence warning inside a protected network.
- Hunt-forward teams seed decoys to draw out an intruder already on the wire.
- Incident responders use planted lures to observe attacker behavior in a controlled space.

04 · COMMERCIAL & ENTERPRISE

- Banks and financial services can watch for lateral movement and credential theft inside segmented networks.
- Critical-infrastructure and operational-technology operators can watch segments no user should enter.
- Managed security service providers can run deception campaigns as a monitored service.

05 · OUTCOMES

- Interaction with a decoy or breadcrumb produces a high-confidence, low-noise alert.
- Adversary contact is captured with context and forwarded into existing analyst workflows.
- Emulated intrusions can be run against the decoys from the deception platform to rehearse detection.

06 · CONSIDERATIONS

- The deception platform is a commercial product, optional and licensed separately.
- Decoy hosts are deliberate bait and are kept isolated; they are not hardened production assets.
- Breadcrumb alerting depends on the host agent running where the lure is planted; plan placement accordingly.

INTEGRATED TOOLS

CounterCraft COMMERCIAL | MITRE Caldera

Commercial products licensed separately · Trademarks of their owners; no endorsement implied