

TREACLE TECHNOLOGIES® i-MIRAGE SYSTEM™ DECEPTION SYSTEM

'In the art of war, deception is often the greatest weapon'
- Chanakya

CORE FUNCTIONAL INSIGHTS

Treacle i-Mirage™ is an AI-Powered deception system that transforms traditional threat detection into a proactive and adaptive defense strategy. At the core of the platform is a dynamic deployment engine that scatters high-fidelity decoys across IT, OT, IoT, and cloud environments, each capable of emulating real services and devices. These decoys, indistinguishable from production systems, engage adversaries early and provide granular behavioral telemetry for threat analysis.

The system leverages machine learning and rule-based orchestration to identify adversaries' intent and dynamically adjust the deception environment, morphing banners, rotating credentials, and deploying contextual mirage networks based on the evolving TTPs.

Unlike earlier deception solutions, i-Mirage™ operates independently of production systems using a fully agentless, non-intrusive model. It captures payloads, session logs, and metadata, transforming them into MITRE-mapped threat intelligence with near-zero false positives. Alerts are pushed in real-time to SIEM/SOAR stacks, enabling accelerated and automated incident response. i-Mirage™ also features a custom offline Generative AI model that integrates with the network and deception data, thereby reducing the Turn Around Time (TAT) of SOC Analysts.

With support for IT, OT, IoMT, and SCADA architectures, i-Mirage™ offers a modular deployment framework that adapts to hybrid and air-gapped networks, ensuring consolidated threat visibility across all layers.

KEY CAPABILITIES OF TREACLE i-MIRAGE™

AI-Driven Proactive Deception

High-Interaction Decoy Emulation

Cyber-Mines and Lures

Real-Time Threat Playbook Generation

Integrated Malware Capture Unit

Agentless and Scalable Architecture

Self-Healing Decoy Capability

Behavior-based Quantified Threat Scoring and Recommendation Engine

Seamless Integration with existing solutions

TECHNOLOGICAL ADVANTAGES

Container-Based Decoy Architecture

All components run as Docker containers, allowing rapid scaling, modular updates, and isolated execution across IT and OT environments

Behavior-Adaptive Deception Engine

Automatically adjusts decoy selection and configuration in response to adversaries' behavior, including scanning, enumeration, and exploitation attempts

Self-Healing Decoy Environment

Each decoy is protected by snapshot-based rollback, enabling full recovery after compromise while preserving forensic evidence

Live Payload Capture and Analysis

Captures injected payloads such as reverse shells, ransomware, and web-based exploits for in-depth forensic and threat intelligence correlation

Multi-VLAN Threat Redirection

Supports traffic redirection from real network zones to deception zones across VLANs and network segments, ensuring safe containment

Real-Time Decoy Permutation

Dynamically alters decoy characteristics such as ports, credentials, and banners during an attack to maintain realism and prolong engagement

Integrated Threat Scoring System















Evaluates adversaries' behavior in real-time using parameters like dwell time, lateral movement, and TTPs to assign risk scores, recommendations, and trigger response actions

Customized OT and SCADA Simulation

Emulates critical industrial protocols such as Modbus, MQTT, FTP, and SMB to create believable OT deception environments

TECHNOLOGICAL SPECIFICATIONS

Key Features & Specs

|  USER DATA CENTRIC DECOY-DOCS & LURES |  APPLICATION-BASED DECOYS |  SUPPORTED OPERATING SYSTEMS |  SUPPORTED DEPLOYMENT PLATFORMS |
|---|---|---|--|
| Honeycredentials <ul style="list-style-type: none"> Fake usernames and passwords embedded in- <ul style="list-style-type: none"> Config files, Backup folder Exposed services Database scripts VPN credentials FTP credentials Deceptive Documents & File Lures <ul style="list-style-type: none"> Fake MoUs Contracts Research papers Password files Config files Source code README folders Backup folders Decoy-Docs Behavioral & Contextual Lures <ul style="list-style-type: none"> Fake databases Transaction logs Payment history Admin portals Phantom APIs Hidden endpoints Internal breadcrumbs VPN breadcrumbs | Web & API <ul style="list-style-type: none"> HTTP/HTTPS Local File Inclusion (LFI) Cross-Site Scripting (XSS) SQL Injection (SQLi) Remote Code Execution (RCE) DNS, SMTP, LDAP Access & Credential-Based <ul style="list-style-type: none"> SSH FTP RDP VPN Active Directory (AD) CoreStack <ul style="list-style-type: none"> SMB MODBUS PRINTER OT Honeypot Data & File System Decoys <ul style="list-style-type: none"> Database Decoy Decoy-Docs Honeytokens Malware Trap <ul style="list-style-type: none"> Octopus Decoy HTTP Malware CapturingDecoy |     |       |

ABOUT TREACLE TECHNOLOGIES

Treacle Tech is a deep-tech cybersecurity company and a recipient of prestigious grants from:

MeiTY TIDE GTM 2.0

DST (Department of Science & Technology)

DoT (Department of Telecommunications)

Startup India Seed Fund (SISFS)

Our vision is to build indigenous deception and cyber-defense technologies that protect critical infrastructure and sensitive networks from targeted cyber threats

Offices: Gurugram, IIT Kanpur

Website: www.treacletech.com

Email: contact@treacletech.com

Phone: +91 8420407686