USP

Treacle Tech
Security, Trust, Assurance

TREACLE TECHNOLOGIES
REDEFINING CYBERSECURITY THROUGH INTELLIGENT DECEPTION

worms HACKERS
DATA VIRUSES USB SPAM
filters
MALWARE phishing botnets
DDOS ATTACKS
FRAUD
COMPLIANCE
ONLINE
scrubbing
BOGONS
TROJANS
webmail
facebook
KNOWLEDGE portable media PRIVATE INFORMATION PATCHES E-MAIL ATTACHMENTS extortion
CYBERBULLYING DESTRUCTION
confidentiality AUTHORIZATION
REDACTION
SPYWARE
WEB exploitation authentication ANTI-SPYWARE
P2P FILE SHARING records accountability CRACKING BROWSING
virtual private networks FRAUD ONLINE SHOPPING
SOCIAL ENGINEERING PRIVACY
integrity espionage REMEDIATION
scrubbing cybercrime BOGIES
IDENTITY THEFT AUTOMATIC UPDATES
strong passwords FIREWALLS
ANTIVIRUS digital copyrights
TROJANS automatic updating CYBERSTALKING social networking
PREDATORS THEFT DANGER online banking
HTTPS CYBERCRIME
INFORMATION SECURITY

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

USP OF TREACLE I-MIRAGE SYSTEM

Real-Time AI-Driven Behavioral Deception Engine

Treacle's i-Mirage™ system leverages an AI-powered behavioral adaptation engine that evolves decoy profiles in real time based on adversaries' TTPs (Tactics, Techniques, and Procedures) and provide risk scoring derived from live network telemetry. This allows the platform to:

Modify deception environments dynamically.

Generate adversary-specific decoy environments on the fly.

Increase the attack cost of the adversary by engaging them over an extended period.

Built for Multi-Zone Security (IT, OT, IoT, Air-Gapped)

Treacle's hybrid deception fabric is purpose-built to operate across traditional IT networks, industrial OT networks, and even isolated air-gapped infrastructures. It supports:

SCADA and ICS protocol emulation.

IoT and smart infrastructure decoying.

Legacy device mimicry without compromising production systems.

Malware Capturing & Reverse Shell Analysis via Octopus

Proprietary Octopus decoy logs and isolates malware deployed through reverse shells.

Supports more than 15 protocols (SMB, SIP, TFTP, MQTT, etc.) and provides full payload behavior analysis.

This is unmatched in scope and depth by competitors such as Smokescreen, or Acalvio.

LLM-Powered Analyst Console

A unique interface backed by large language models enables SOC analysts to interact with attack logs, decoy events, and forensic data using plain English. This natural language-driven approach:

Significantly enhances the efficiency and effectiveness of security operations.

Empowers junior analysts to perform threat hunting and investigation at an expert level.

Offers a capability currently unmatched in the honeynet and deception technology space.

Adaptive Cyber Mines with Proactive Threat Engagement

i-Mirage deploys "cyber mines"—silent decoys that trigger only under suspicious reconnaissance. These:

Are placed in unused IPs across VLANs

Adapt engagement rules based on observed threat patterns

Mimic enterprise systems like payment gateways, Active Directory, or VPNs

This provides a zero false positive early warning system an industry first

Behavioral Threat Scoring and Risk-Adaptive Deception

Treacle employs real-time risk scoring using AI models to:

Modify honeypots dynamically based on attacker behavior

Prioritize threats by intent and sophistication

Escalate from passive to active deception based on real engagement patterns

Full Spectrum Attack Lifecycle Coverage (MITRE-Aligned)

Treacle has proven capability to detect and engage across multiple MITRE ATT&CK stages, including:

Initial Access

Execution

Credential Access

Lateral Movement

Exfiltration

With active logging, payload capture, and attacker replay sessions

Self-Restoration Deception Architecture

Once compromised, decoys automatically roll back to a clean state, preventing reuse or lateral escalation.

Eliminates the need for manual reconfiguration.

Extremely Low False Positive Rate

Because alerts are generated from decoy interactions, they inherently signal malicious intent.

Threat Actor Attribution and Geo Intel

Unlike conventional security platforms, Treacle captures:

VPN and Tor usage analysis.

Abuse scoring of IP addresses.

Origins and behavior of reverse shell activity.

This enables deep, real-time threat actor profiling that goes far beyond basic indicator-based detection.

Seamless Air-Gapped & Zero Trust Integration

i-Mirage™ is purpose-built to support:

Fully isolated, air-gapped environments with no internet dependency.

Zero Trust security models, where every access request is verified, across a wide range of IT, OT, and cloud systems.

High-precision threat detection with minimal false positives, surpassing the limitations of traditional behavioral tools.

Custom Threat Intelligence and Organization-Specific Insights

i-Mirage™ builds a real-time threat intelligence graph specific to the deployed environment. It captures:

Adversary toolkits and malware variants unique to the organization.

Movement patterns used by adversaries to navigate across internal networks, segments, or systems.

Behavioral profiles for adversary fingerprinting.

Unlike generic TI feeds, this is personalized, contextual, and immediately actionable.

Seamless Integration and Minimal Hardware Footprint

Built on a modular, agentless architecture.

Designed with an API-first approach for easy integration into existing security ecosystems.

Requires no changes to network infrastructure or additional hardware deployment.

Proven Cost-Efficiency and Exceptional ROI

Treacle deployments have consistently delivered outstanding return on investment across a range of industries. This impact is driven by:

Substantial reduction in breach response and remediation costs.

Enhanced efficiency and focus for SOC teams through high-fidelity, actionable alerts.

Lowered compliance exposure by intercepting threats at the earliest possible stage.

Autonomous Threat Response and Orchestration

Real-time orchestration of decoys across multiple VLANs, triggered by reconnaissance or anomalous behavior.

Requires minimal manual intervention for deployment; reacts autonomously using ML + rule-based models.

Zero-Day Threat Identification Without Known IOCs

Detects threats during the reconnaissance phase, even in the absence of indicators of compromise.

Especially effective for APTs, ransomware pre-execution phases, and novel botnet/DDoS attacks.

Custom Decoy Generation

Generates decoys mimicking real applications (banking apps, ERPs, OT systems).

Decoys can be customized for specific CVEs or service configurations based on observed adversaries' behavior.

Granular, Multi-Layered Analytics Dashboard

Includes filters by decoy type, subnet, protocol, country, and time window.

Offers command analysis, credential tracking, protocol attack radars, geolocation, fraud scores, and adversary origin analytics.

Real-Time Threat Map and Incident Replay

Tracks live adversaries' movement visually, offering replay of incidents for forensic analysis and legal evidence.

Seamlessly integrates into existing security infrastructure.