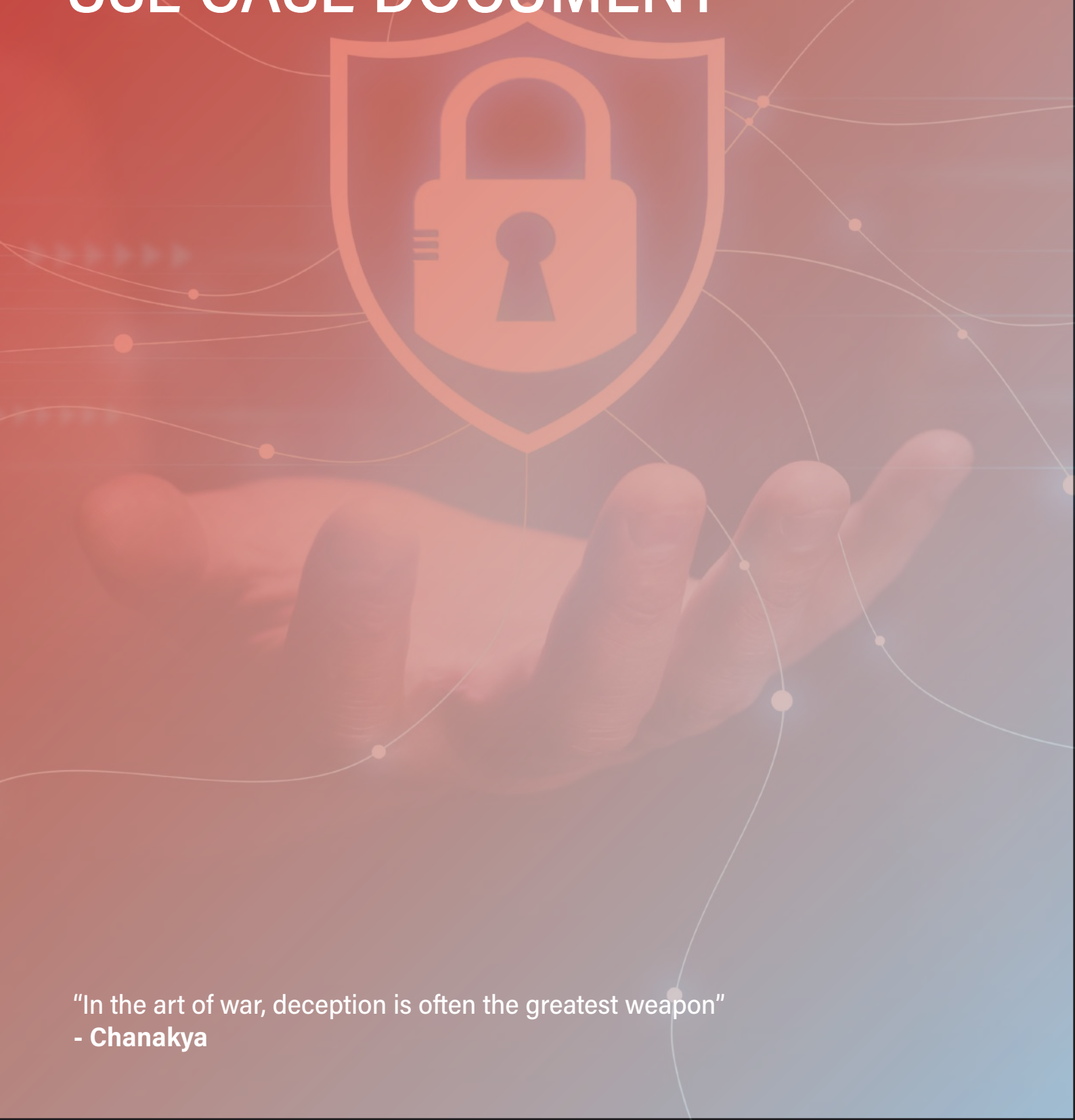
USE CASES

Treacle Tech
Security, Trust, Assurance

TREACLE TECHNOLOGIES
USE CASE DOCUMENT



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

Treacle Tech
Security, Trust, Assurance

EARLY THREAT DETECTION

Use Case

Identify adversaries', during reconnaissance to break the cyber kill chain.

How

The Treacle i-Mirage™ system deploys highly interactive, AI-powered decoys and cyber mines across the network. These decoys are indistinguishable from real systems and are specifically designed to remain invisible to legitimate users. When an adversary intrudes into the network, probes services, or attempts unauthorized access, these deceptive elements respond in realistic ways. Any interaction with them is treated as a clear sign of malicious intent, as legitimate users would never encounter or engage with them. This allows the system to detect the presence of an adversary before they can reach critical assets or crown-jewel systems.

DETECT MALICIOUS USER BEHAVIOR

Use Case

Identify users exhibiting suspicious or unauthorized behavior within the network, whether they are malicious insiders or external adversaries using stolen credentials.

How

The Treacle i-Mirage™ system deploys realistic decoys that replicate high-value enterprise resources such as financial applications, database servers, document repositories, and administrative portals. These decoys are placed strategically across the network but remain invisible to authorized users following normal access patterns. Any user who discovers and attempts to interact with these decoys is almost certainly acting outside the boundaries of their intended role or privilege level. This includes employees misusing access, external adversary with compromised credentials, or automated tools performing reconnaissance. Each interaction is treated as a behavioral anomaly and is reported in real-time for immediate review and response.

Benefit

Organizations gain the ability to detect malicious behavior early in its lifecycle, even when it originates from trusted identities or seemingly legitimate accounts. This reduces the risk of internal data theft, privilege escalation, or advanced persistent threats moving undetected within the network. Security teams receive high-confidence alerts that minimize false positives and provide the necessary context to respond swiftly and contain potential damage.

Treacle Tech
Security, Trust, Assurance

TARGETED MALWARE CAPTURE

Use Case

Intercept advanced or previously unknown malware variants that are specifically designed to bypass conventional security systems and target enterprise environments

How

Treacle i-Mirage™ deploys high-interaction malware-capturing decoys, such as the Octopus decoy, which are configured to mimic vulnerable services frequently targeted by malware, including FTP servers, SMB shares, and HTTP endpoints. These decoys are designed to mimic real systems with real configurations, attracting adversaries and targeted malwares designed to exploit such weaknesses. When the targeted malware is deployed in these decoys, the system captures the payloads in a controlled environment and records the methods used for delivery and execution. This allows for detailed forensic analysis and reverse engineering of the malware without any risk to production systems.

Benefit

By capturing live and evolving malware strains in the wild, organizations gain access to intelligence that is often unavailable through traditional antivirus, endpoint detection tools, and existing SOC. This enables faster identification of zero-day threats, improves defensive posture through signature and behavior analysis, and allows for better-informed threat hunting and response efforts.

LATERAL MOVEMENT DETECTION

Use Case

Detect and isolate adversaries who attempt to move across systems within the network after gaining an initial foothold

How

Treacle i-Mirage™ introduces deceptive systems and services throughout segmented parts of the network including IT infrastructure, industrial control systems, and IoT environments. These decoys are embedded within normal communication paths and replicate actual systems, making them appear as legitimate targets to an adversary attempting to pivot from one host to another. When an adversary uses techniques like credential harvesting, remote command execution, or privilege escalation to explore or compromise additional systems, the decoys capture these actions and generate alerts with detailed telemetry. This information includes adversaries' movement patterns, tools used, and privilege levels attempted.

Benefit

Security teams can detect lateral movement before the adversaries reach sensitive systems or complete their objectives. The alerts are high-confidence and provide rich context for threat response platforms such as SIEM and SOAR, enabling swift containment of the threat and comprehensive incident resolution.

Treacle Tech
Security, Trust, Assurance

SOC OPTIMIZATION AND ALERT REDUCTION

Use Case

Improve the efficiency of Security Operations Center teams by minimizing false positives and focusing analyst attention on verified threats.

How

The Treacle i-Mirage™ system generates alerts only when a user or adversary interacts directly with a deception asset. These assets are invisible and inaccessible to legitimate users under normal conditions, which means any engagement is treated as a confirmed threat. This eliminates the guesswork and investigation required to validate alerts from traditional systems. Each alert is enriched with context such as adversary behavior, protocol used, and targeted asset type, and is forwarded directly to existing cybersecurity monitoring and response systems for triage and prioritization.

Benefit

By surfacing only high-confidence incidents, the system dramatically reduces the volume of noise that SOC analysts must manage. This leads to a measurable improvement in incident handling speed, analyst productivity, and overall, SOC effectiveness. In real-world scenarios, organizations have reported more than a 50 percent improvement in operational efficiency after integrating i-Mirage™ into their security workflow.

AIR-GAPPED AND OT/IOT ENVIRONMENT

Use Case

Enable effective threat detection and early warning capabilities within isolated or air-gapped operational technology /Internet of Things environments.

How

Treacle i-Mirage™ includes decoy assets specifically designed for OT/IoT networks, including systems that emulate industrial control protocols such as Modbus, MQTT, SMB, and others commonly found in SCADA environments. These decoys are deployed inside segmented and even air-gapped networks where traditional security tools cannot operate due to safety, performance, or compatibility concerns. The decoys simulate critical industrial devices and processes, capturing reconnaissance, unauthorized access attempts, and command injection attacks without interfering with actual operations.

Benefit

This allows organizations to introduce a layer of active defense into highly sensitive infrastructure without risking down-time or compliance issues. By detecting threats within environments that are otherwise blind to modern monitoring tools, the system plays a vital role in protecting critical infrastructure and supporting national cybersecurity mandates.

Treacle Tech
Security, Trust, Assurance

COMPLIANCE AND FORENSICS

Use Case

Ensure that cybersecurity operations meet regulatory and audit requirements such as PCI-DSS, GDPR, SEBI and RBI Cybersecurity Guidelines.

How

Treacle i-Mirage™ continuously records all adversaries' interactions with decoys, generating immutable audit logs, timestamped alerts, and detailed behavioral records. These logs are maintained in a tamper-resistant format and support forensic replay of incidents for root cause analysis and compliance reporting. Security teams can extract documented evidence of breach attempts, including IP data, payloads, and attempted access paths, to demonstrate adherence to detection and response protocols.

Benefit

The system provides verifiable evidence of security controls in action, helping organizations pass audits, reduce regulatory penalties, and maintain strong governance. It also improves the ability to respond to breach inquiries with detailed and defensible records.

ADAPTIVE THREAT INTELLIGENCE

Use Case

Generate actionable threat intelligence based on real-time adversaries' behavior to enhance defensive strategies and incident response.

How

Treacle i-Mirage™ integrates an AI engine that dynamically adjusts deception profiles based on adversary tactics observed during live engagements. This includes mapping adversaries' behavior to frameworks like MITRE ATT & CK and modifying decoy configurations accordingly. The system adapts to engagement duration, exploited vulnerabilities, and attack frequency, creating customized deception environments that evolve with the threat landscape.

Benefit

The continuous learning and adaptation process creates a self-healing deception layer that not only detects threats but also strengthens itself over time. This reduces vulnerability windows, improves threat-hunting accuracy, and aligns defensive posture with current adversary techniques.

Treacle Tech
Security, Trust, Assurance

REMOTE OFFICE AND LEGACY SYSTEMS PROTECTION

Use Case
Extend cybersecurity coverage to remote locations and legacy systems that may not support modern security solutions.

How
The i-Mirage™ system enables lightweight, agentless deployment of decoys in environments with limited infrastructure, such as branch offices or outdated systems. These decoys simulate local servers, services, and endpoints and are fully operational without requiring heavy hardware or cloud dependencies. They are integrated into local networks to detect unauthorized scanning, lateral movement, or exploitation attempts, even in systems that cannot run endpoint protection.

Benefit
Organizations gain deception-based protection across distributed and vulnerable assets without significant overhead or architectural change. This helps unify the security posture across the entire IT and OT landscape, regardless of technical limitations.

HIGH-VALUE ASSET AND INTELLECTUAL PROPERTY

Use Case
Prevent adversaries from gaining access to business-critical systems and intellectual property such as databases, source code repositories, and financial platforms.

How
Treacle i-Mirage™ places decoys that closely replicate the look, structure, and behavior of sensitive assets around actual critical systems. These decoys act as first-touch targets for adversaries, diverting them away from production systems and capturing detailed telemetry on their techniques. The engagement environment is designed to hold the adversaries attention while relaying threat details to incident responders in real time.

Benefit
The system serves as an active buffer zone around high-value infrastructure, increasing the likelihood of early detection and reducing the risk of data theft, espionage, or sabotage. At the same time, it provides intelligence about what adversaries are targeting and how.

PHISHING AND COMMAND-CONTROL DETECTION

Use Case
Identify and analyze phishing campaigns and malware infections that attempt to establish command-and-control communication with external servers.

How
Treacle's Octopus decoy is engineered to detect and intercept malicious payloads delivered through phishing emails, reverse shells, or automated network injections. When a payload is deployed, the system captures all associated activity, including attempts to communicate with external command-and-control (C2) servers. It logs the destination addresses, communication protocols, and timing patterns, enabling forensic teams to trace the infrastructure being used by adversariess.

Benefit
Organizations gain the ability to isolate phishing-based intrusions and understand how adversaries control infected endpoints. This intelligence supports the blocking of external C2 infrastructure, improves incident response accuracy, and contributes to threat feed enrichment and source attribution.

BEHAVIORAL PROFILING OF ADVERSARIES

Use Case
Develop in-depth behavioral profiles of adversaries based on their live interaction with decoy systems.

How
The i-Mirage™ system records detailed metadata from every adversary's interaction, including command sequences, reverse shell behavior, injected payloads, credential usage, and exploitation techniques. These behaviors are mapped to threat frameworks such as MITRE ATT&CK and cross-referenced with known threat intelligence sources. Over time, the system builds adversaries-specific behavioral signatures and intent-based profiles, highlighting their preferred tactics, tools, and objectives.

Benefit
This profiling enables more accurate attribution, strengthens threat hunting efforts, and allows for adaptive defensive strategies. By understanding how different adversaries' groups operate, security teams can prepare tailored countermeasures and enhance detection capabilities across the network.

Treacle Tech
Security, Trust, Assurance

ADAPTIVE INCIDENT CONTAINMENT

Use Case
Proactively contain and neutralize active threats by isolating adversaries in controlled deception environments before they can cause damage.

How
Treacle i-Mirage™ engages adversaries in isolated decoy systems that mimic production assets but are logically segmented from real infrastructure. As adversaries interact with these decoys, the system evaluates threat severity and automatically triggers containment actions through SOAR integrations. This includes blocking the adversaries' IP address. The containment logic adapts dynamically based on the adversaries' behavior, ensuring the response is both timely and appropriate.

Benefit
This capability buys critical time for security teams to investigate and respond, while simultaneously limiting the adversaries' ability to pivot or escalate privileges. It reduces the blast radius of successful intrusions and transforms detection into active defense.

AI-POWERED THREAT ENGAGEMENT AND SOAR INTEGRATION

Use Case
Use artificial intelligence to dynamically adjust deception deployment and automate coordinated security responses.

How
Treacle i-Mirage™ incorporates an AI engine that analyzes adversaries' behavior in real- time, such as their movement patterns, exploitation methods, and interaction depth. Based on this analysis, the system dynamically reconfigures decoys to prolong adversaries' engagement and improve realism. Simultaneously, it integrates with SOAR platforms to automate response workflows like alert escalation, IP blocking, or sandbox analysis. The entire process adapts continuously to reflect the sophistication and intent of the adversaries.

Benefit
This closed-loop system increases adversaries' dwell time within decoys, reduces manual workload for analysts, and enables rapid, intelligent containment of emerging threats. It enhances both the detection and response capabilities of the organization.

Treacle Tech
Security, Trust, Assurance

DECOY ENGAGEMENT FOR MULTI-STAGE APTS

Use Case
Detect, engage, and analyze long-dwell Advanced Persistent Threats (APTs) that progress through multiple phases of attack over time.

How
Treacle i-Mirage™ deploys high-fidelity honeynets that simulate complete organizational environments, including IT, OT, and user endpoints. These honeynets replicate authentic system behavior and workflows, making them ideal for capturing APT activity across all stages—initial reconnaissance, exploitation, lateral movement, persistence, and data exfiltration. The system monitors adversaries' behavior throughout their engagement, logging every action for analysis while keeping the adversaries contained within a controlled environment.

Benefit
Security teams gain full visibility into the tactics, techniques, and procedures (TTPs) used by sophisticated adversaries. This insight helps identify defensive gaps, refine threat models, and build targeted countermeasures to prevent future attacks.

ADVANCED DECOY CUSTOMIZATION AND ANALYTICS

Use Case
Customize and fine-tune deception strategies to match specific attack surfaces and network environments.

How
The i-Mirage™ platform allows users to configure decoys for specific services such as SSH, SQLi, HTTP, and RDP. It provides filtering options to focus on individual protocols, timeframes, or attack vectors, and enables exporting of analytics reports in formats suitable for sharing and review. This flexibility ensures that security teams can tailor decoy deployment and analysis to match the organization's risk profile and infrastructure layout.

Benefit
Targeted decoy customization and protocol-level monitoring increase the relevance and effectiveness of deception efforts. Security teams gain deeper insights into how specific assets are being targeted, enabling more precise detection and response.