Thinkst Canary Deception Deployment & Optimisation for UK Public Sector Consultancy

Service Overview

We help UK public sector organisations cut through the noise of modern cyber threats and augment detection capabilities by deploying Thinkst Canary deception technology—specifically designed to catch attackers before they reach your crown jewels.

We deploy realistic, embedded decoys that trigger only when attackers interact with them – giving you earlier, higher-fidelity detection of malicious activity before they compromise your data. We enable you to detect lateral movement, credential theft, and stealthy intrusions faster, with less alert fatigue.

Capabilities

Strategic Design & Architecture:

- Assess your estate: Map high-risk zones (e.g., cloud storage, AD domains, critical services) using your NCSC risk framework and asset classification.
- Deploy decoys that blend in: Canary tokens (fake credentials), decoy servers (mimicking your actual services), and cloud resources – all designed to avoid triggering false positives from internal users.
- Align with your threat model: Placement prioritised by your actual risk profile (e.g., targeting credential theft paths identified in your annual threat assessment).Deployment and configuration

Seamless Integration with Your SOC:

- Canary alerts feed directly into your SIEM, SOAR, and ticketing systems.
- We configure alert severity, enrichment (e.g., linking to your asset database), and escalation paths to match your existing playbooks.

Optimisation & Continuous Value:

- Quarterly health checks: Review decoy effectiveness, remove low-value assets, and adjust for infrastructure changes.
- Threat-adaptive tuning: Update decoy behaviour based on emerging threats, using threat intelligence.
- Embed in BAU: Provide runbooks for SOC teams and platform owners, ensuring deception becomes part of routine operations.

Knowledge Transfer:

- Tailored training: Hands-on sessions for SOC analysts on interpreting and triaging Canary alerts.
- Documentation: Clear, classified-ready guides for incident response, including how to validate alerts against your asset inventory.
- Knowledge transfer: All designs, configurations, and runbooks will be handed over to you.

Benefits and outcomes

- High-fidelity early-warning: Gain earlier, clearer visibility of attackers performing lateral movement, credential theft, or reconnaissance—before they touch your real “crown jewels”.
- Noise reduction: Reduce noise by focusing on high-confidence, low-volume alerts that indicate genuinely suspicious behaviour rather than routine operations.

© 2T Security Ltd 2026

- Value maximisation: Maximise the value of your existing SIEM, SOAR, and logging platforms by feeding them rich, contextual Canary alerts instead of adding yet another isolated tool.
- Integration into existing SOC: Enhance existing detection and response capabilities without needing to re-architect your security stack.
- Rapid time-to-value: Move from concept to operational deception quickly through structured design, deployment, and tuning support that avoids common implementation pitfalls.
- Documentation and knowledge transfer: Shorten the learning curve for teams new to deception technologies through practical training and embedded playbooks.

Onboarding and Offboarding / Engagement Process

Onboarding:

- Discovery and scoping: Run workshops with security, IT, and business stakeholders to understand your estate, threats, objectives, and constraints, including any regulatory or classification requirements.
- Design: Produce a high-level and low-level design for Canary deployment, including bird/token placement, naming conventions, integration points, and alert flows.
- Implementation: Support or lead deployment and configuration, integrating Canary with your SOC tooling and testing alert flows end-to-end.
- Validation and handover: Execute test scenarios, refine tuning, and hand over with documentation, training, and agreed operating procedures.

Offboarding / end of engagement:

- Final review: Conduct a closing review of the deployment, confirming ownership, responsibilities, and any outstanding recommendations.
- Asset and access hand back: Transfer all configuration artefacts and documentation to your repositories and remove any temporary consultancy access.

Security

Personnel and clearances:

- Consultants are vetted to appropriate UK government standards (e.g. BPSS as a baseline), with higher clearances available where required by the buyer.
- Work is delivered in line with your organisational security policies, access controls, and change-management processes.

Data protection and classifications:

- The service is designed for environments handling data up to and including OFFICIAL and OFFICIAL-SENSITIVE, with designs and processes aligned to your information-assurance requirements.
- Any access to logs, configurations, or management consoles is controlled, auditable, and time-bound, with least-privilege applied.

Secure ways of working:

- Use of secure communication channels, secure storage of engagement artefacts, and appropriate segregation of customer environments.
- Clear definition of roles and responsibilities for managing Canary in production, ensuring that deception capabilities remain effective, controlled, and trusted by stakeholders.

© 2T Security Ltd 2026