Canaries and honeytokens: would you know an intruder is already inside?

This month, plant decoys on the paths intruders take first, such as a Kerberoastable honeytoken account, a fake password file on a share and fake cloud keys on admin and developer machines, and route every trip to whoever handles high-severity alerts at night. Treat each trip as an intrusion until you can name the person or tool that caused it.

Reviewed	Next review	Version	Written for
5 Nov 2026	**5 Dec 2026**	**1.0**	**IT and security teams in small and mid-size organizations, especially on Active Directory, Microsoft 365 and AWS**

Latest version
sheets.einblick.dev/deception/

If you only do five things

1. **Put decoys where intruders already look.**
   Attackers request service tickets for accounts with a service principal name (SPN) and crack them offline[1], and search shares for stored passwords[2]. A honeytoken account with an SPN and a fake password file catch both.
2. **Send every trip to someone who acts at night.**
   Route them like the logging sheet's alerts, to a named owner and deputy. Ask your MDR provider in writing whether it acts on them: Microsoft's Defender Experts covers only High and Medium incidents, not custom detections[3].
3. **Build on tools you already run.**
   Defender for Identity, Windows auditing, CloudTrail and Microsoft 365 alert policies keep alert data in systems you control. Decoys work: in a test with over 130 red teamers, everyone facing decoy hosts set one off before reporting a successful exploit[4].
4. **Trip each canary yourself.**
   Test it when placed and every quarter, timing the alert until a person answers. Microsoft 365 alert policies take up to 24 hours to start[5], and Key Vault logs can lag up to 10 minutes[13].
5. **Keep a register and tell almost no one.**
   Record each decoy's location, trigger and alert path for the few admins who need it, so nobody uses or deletes one by mistake. In the NCSC's trials, 90% of participants said they wouldn't publicly announce using deception[6].

Plant your first decoys

1. **A honeytoken account in Active Directory.**
   Create an unused user with an attractive name, an SPN, a long random password and no rights. Tag it **Honeytoken** in Defender for Identity (Microsoft 365 E5, E5 Security, EMS E5 or standalone[7]) to alert on its sign-ins, LDAP lookups and changes[8]. Either way, alert on event 4769 for the account, which needs **Audit Kerberos Service Ticket Operations** on domain controllers[9].
2. **A password file on a share.**
   List the honeytoken in it and audit reads with **Audit File System** and a SACL: Windows then logs event 4663 with the account and process[10]. In SharePoint, alert on **Accessed file** for its URL[5]; `app@sharepoint` hits are often retention policies[11].
3. **Fake cloud keys.**
   Create an IAM user without permissions in a separate AWS account; leave its keys on admin and developer machines and in CI. With an active multi-Region trail, set an EventBridge rule in each Region to `ENABLED_WITH_ALL_CLOUDTRAIL_MANAGEMENT_EVENTS`, or it misses read-only calls[12].
4. **A decoy secret and a decoy cloud user.**
   With Key Vault logging on, alert on any `SecretGet` for a fake secret[13] and on any sign-in by a decoy Entra ID user, the way Microsoft shows for emergency access accounts[14].
5. **Names only a thief would use.**
   Put a canary hostname in SSH configs, RDP files and runbooks and a unique email address in fake customer and HR records, and alert on lookups and on mail your systems didn't send.

Free, self-hosted or paid

- **canarytokens.org is free, with only an acceptable use policy.** Thinkst runs it as a public service for any lawful purpose, promises only to work hard to keep it running and uses third parties such as Mailgun and AWS[15]. Use it to try token types, not for production.
- **Self-host the open-source server.** Its GPLv3-based license allows internal use; embedding it in proprietary software needs a commercial license[17]. Patch it like any internet-facing server.
- **Decoy hosts.** OpenCanary, BSD-licensed, emulates network services on a small VM; Thinkst Canary is its commercial version[18]. Ask vendors for a data processing agreement.

When a canary fires

1. **Who or what touched it?**
   Check the account, host, IP address and process against the register of backups, scanners and tests.

Germany: works council and data protection

- **Involve the works council first.** It co-determines technical systems designed to monitor employees' behavior or performance, and the Federal Labor Court counts any system objectively suitable for that, whatever the employer intends[19]. A decoy that logs which account opened it qualifies.
- **Put the rules in a works agreement.** Cover what is logged, who sees alerts, retention and that trips aren't used to judge performance.
- **Mark placements as confidential.** Works council members may not disclose business secrets the employer expressly marks as confidential[20].
- **Ask your data protection officer about external services.** Alerts can identify staff, and the GDPR requires a contract with any processor[16].

Mistakes that cost the most

- **A decoy that unlocks something real.** A honeytoken with a weak password or real rights becomes a way in. Use a long random password, no extra groups and a Conditional Access block on Entra ID sign-in.
- **Canary keys in public repositories.** GitHub reports partner secrets found in public repositories to the provider, which may revoke them or contact you[21]. Keep keys where only an intruder looks.

2. **Treat an unexplained trip as an intrusion.**
   Follow the incident response sheet: isolate without wiping and export the logs. Leave the decoy in place, or the attacker learns they were seen.
3. **Reset what was within reach.**
   Reset the account that tripped it and every credential near the decoy, in one coordinated round if admin rights are at risk. If a canary key was used, treat its machine as compromised.
4. **Record the cause.**
   If your own tool tripped it, move the decoy instead of excluding the tool.

What changed in 2026

- **The UK tested deception at scale.** In December 2025 the NCSC reported on an experiment with 121 organizations: most saw potential value in detecting novel threats, but misconfigured tools can miss threats, give false confidence or create openings for attackers[6].
- **Defender for Identity got easier to switch on.** Since October 2026, its v3.x sensor runs on domain controllers without Defender for Endpoint, and turns on by itself where Defender for Endpoint runs, unless you opt out[23].
- **Sign-in page canaries are ending.** Thinkst's Entra ID token, which flags proxied sign-in pages, needs custom CSS branding[24]. Tenants without it can't add it after 21 July 2026, and Microsoft will retire it[25].

What you can skip

- **Internet-facing honeypots.** They tell you about the internet's scanners, not about your network. Put decoys inside.
- **Fake environments that engage intruders.** Decoy accounts, files and keys are enough to detect an intrusion.
- **Hundreds of decoys before five work.** Deception needs tuning as networks change[6]. Grow only as fast as you test.
- **A deception platform before an on-call rotation.** If nobody answers a High alert at night, a canary alert waits too (see the SOC and MDR sheet).

What this looks like at your size

Small team, no security staff

- Put a fake password file in SharePoint with an alert policy on **Accessed file**[5]; check that your plan allows custom alert policies.
- Leave fake cloud keys on the admin laptop if you use AWS.
- Send alerts to two people's phones and trip every decoy each quarter.

Growing, with IT or security staff

- Alert on event 4662 for AD canary objects that nobody may read[1]; audit tools trip them too.
- Self-host Canarytokens, or buy a product with a data processing agreement.
- Agree canary handling with your MDR provider and works council.

Enterprise or regulated

- Place decoys in each tier and network zone, including management, OT and cloud accounts.
- Report trips and time to response with your detection metrics.
- Include decoys in red team scopes and move any that testers walk past.

Version history

5 Nov 2026, version 1.0 Published after a copy edit and a source-by-source fact check, which added the September 2026 joint guide on Active Directory compromise, scoped the red team study to decoy hosts, made AWS and Defender for Identity alerting complete and blocked honeytokens from signing in.

Sources

1. Detecting and mitigating Active Directory compromises. ASD, CISA, NSA and partners, Sep 2026. ncsc.govt.nz
2. Unsecured Credentials: Credentials In Files (T1552.001). MITRE ATT&CK, modified 11 Sep 2026. attack.mitre.org
3. FAQs related to Microsoft Defender Experts MDR. Microsoft Learn, 28 Jul 2026. learn.microsoft.com
4. Examining the Efficacy of Decoy-based and Psychological Cyber Deception. USENIX Security 2021, Aug 2021. usenix.org
5. Alert policies in the Microsoft Defender portal. Microsoft Learn, 3 Aug 2026. learn.microsoft.com
6. Cyber deception trials: what we've learned so far. NCSC (UK), 11 Dec 2025. ncsc.gov.uk
7. Defender for Identity sensor v2.x prerequisites. Microsoft Learn, 8 Jun 2026. learn.microsoft.com
8. Defender for Identity classic security alerts. Microsoft Learn, 16 Aug 2026. learn.microsoft.com
9. 4769(S, F) A Kerberos service ticket was requested. Microsoft Learn, 7 Sep 2021. learn.microsoft.com
10. 4663(S) An attempt was made to access an object. Microsoft Learn, 7 Sep 2021. learn.microsoft.com
11. Audit log activities. Microsoft Learn, 3 Nov 2026. learn.microsoft.com
12. AWS service events delivered via AWS CloudTrail. Amazon EventBridge docs, checked 5 Nov 2026. docs.aws.amazon.com
13. Azure Key Vault logging. Microsoft Learn, 10 Apr 2026. learn.microsoft.com
14. Manage emergency access admin accounts. Microsoft Learn, 4 Jun 2026. learn.microsoft.com
15. Canarytokens Acceptable Use Policy. Thinkst, checked 5 Nov 2026. canarytokens.org
16. Regulation (EU) 2016/679 (GDPR), Article 28. EUR-Lex, 2016. eur-lex.europa.eu
17. Canarytokens LICENSE. Thinkst (GitHub), checked 5 Nov 2026. github.com
18. OpenCanary README and license. Thinkst (GitHub), checked 5 Nov 2026. github.com
19. Decision 1 ABR 16/23, para. 25. Bundesarbeitsgericht, 16 Jul 2024. bundesarbeitsgericht.de
20. Betriebsverfassungsgesetz, § 79. gesetze-im-internet.de, checked 5 Nov 2026. gesetze-im-internet.de
21. About secret scanning for partners. GitHub Docs, checked 5 Nov 2026. docs.github.com
22. How to create and troubleshoot the Windows Folder Canarytoken. Thinkst Canary help center, checked 5 Nov 2026. help.canary.tools
23. What's new in Microsoft Defender for Identity. Microsoft Learn, 28 Oct 2026. learn.microsoft.com
24. Azure Entra ID login token. Canarytokens docs (Thinkst), checked 5 Nov 2026. docs.canarytokens.org
25. Add company branding to your organization's sign-in page. Microsoft Learn, 18 Aug 2026. learn.microsoft.com