Template - Honeytoken activity

Link to alert

**Description**

Honeytoken accounts are decoy accounts set up to identify and track malicious activity that involves these accounts. Honeytoken accounts should be left unused, while having an attractive name to lure attackers (for example, SQL-Admin). Any activity from them might indicate malicious behaviour.

**Classification**: Incident

**How to investigate**

[ATA suspicious activity guide | Microsoft Docs](https://docs.microsoft.com/en-us/advanced-threat-analytics/suspicious-activity-guide#:~:text=Honeytoken%20activity.%20Description.%20Honeytoken%20accounts%20are%20decoy%20accounts,Any%20activity%20from%20them%20might%20indicate%20malicious%20behavior.)

**Alert detail**

Description:

Start Time:

End Time:

Severity:

Source User Account name:

Domain controllers:

**Remediation**

Check whether the owner of the source computer used the Honeytoken account to authenticate, using the method described in the suspicious activity page (for example, Kerberos, LDAP, NTLM).

Browse to the source computer(s) profile page(s) and check which other accounts authenticated from them. Check with the owners of those accounts if they used the Honeytoken account.

This could be a non-interactive login, so make sure to check for applications or scripts that are running on the source computer.

Make sure Honeytoken accounts are used only for their intended purpose, otherwise they might generate many alerts.

***NB: PROVIDE A SCREESNHOT OF THE WORK DONE***