Template - Suspected identity theft (pass-the-ticket)

[Link](https://premierfoodsonline.portal.cloudappsecurity.com/#/alerts/60f55df1055dcc19115256d8) to alert

**Description**

Pass-the-Ticket is a lateral movement technique in which attackers steal a Kerberos ticket from one computer and use it to gain access to another computer by reusing the stolen ticket. In this detection, a Kerberos ticket is seen used on two (or more) different computers.

**Classification**: Incident

**Alert detail**

User:

Date:

Kerberos ticket was first observed:

* Device name:
* IP address:

Kerberos ticket used on:

* Device name:
* IP address:

Kerberos ticket used to log into:

* Device name:

Severity: High

**Remediation**

Contain the Device for the remediation

Check if the IP addresses of the computer does not belong to a subnet that is allocated from an undersized DHCP pool.

Reset the password to a strong password.

Search for the tool that potentially performed that the attack and remove it.

Use klist.exe purge to delete all the tickets of the specified logon session and prevent future usage of the tickets.

