Template - Suspicious authentication activity

Link to alert

**Description**

This resembles a dictionary attack, in which an attacker performs numerous authentication attempts using a dictionary of predefined account names and passwords in order to find valid credentials to access the host. This indicates that some of your host account names might exist in a well-known account name dictionary.

**Incident**: Alert

**Alert detail:**

Top accounts with failed sign in attempts (count):

Activity start time:

Activity end time:

Attacker source IP - IP Address:

Attacker source computer name:

Number of failed authentication attempts to host:

Number of existing accounts used by source to sign in:

Number of non-existent accounts used by source to sign in:

**Accessed Resource**

Device name:

Is domain joined:

IP address:

Last signed in user:

**Suggested Remediation**

Contain the source computer

* Find the tool that performed the attack and remove it.
* Look for users (Jacques Theron) who were logged on around the same time as the activity occurred, as these users may also be compromised. Reset their passwords.
* Set up an NSG allow list of only expected IP addresses or ranges.
* Lock down access to it using network JIT