Demo Correlation Rule

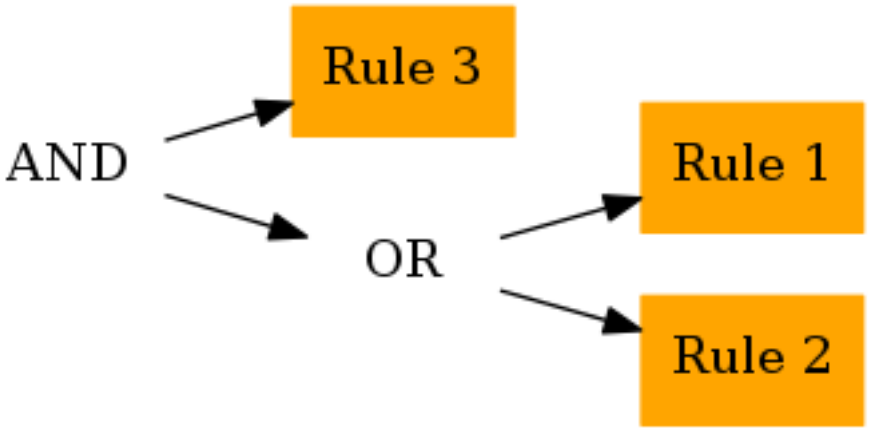
Description

This correlation rule is for demo purposes only. It makes no sense at all and is only needed to test esm2markdown.

General Information

- **Rule ID:** 47-6000112
- **Normalization ID:** 4026531840
- **Severity:** 50
- **Tag:** Demo Correlation Rules
- **Group By:** SRC_ZONE

Correlation Details



Parameters

- **Demo Parameter**
  - **Description:** This parameter is a parameter.
  - **Default Value:** UserIDSrc|6751494449278544611[root]

Rules

Rule 1

- **Activate:** EVENT
- **Match Type:** FILTER
  - **Count:** 1
- **Action:** Trigger
  - **Timeout:** 600
  - **Time Units:** SECOND
  - **Threshold:** 5
- **Match Filter**
  - **Filter Component**
    - **Condition:** 'SRC_IP' EQUALS '1.1.1.1'

Rule 2

- **Activate:** EVENT
- **Match Type:** FILTER
  - **Count:** 1
- **Action:** Trigger
  - **Timeout:** 600
  - **Time Units:** SECOND
  - **Threshold:** 5
- **Match Filter**
  - **Filter Component**
    - **Condition:** 'CUST_4259873' EQUALS 'Description|12622590293378144023[bla]'

Rule 3

- **Activate:** EVENT
- **Match Type:** FILTER
  - **Count:** 1
- **Action:** Trigger
  - **Timeout:** 600
  - **Time Units:** SECOND
  - **Threshold:** 1
- **Match Filter**
  - **Filter Component**
    - **Condition:** 'CUST_2' EQUALS 'CommandID|6751494449278544611[$var=PRIVILEGED_USERS]'