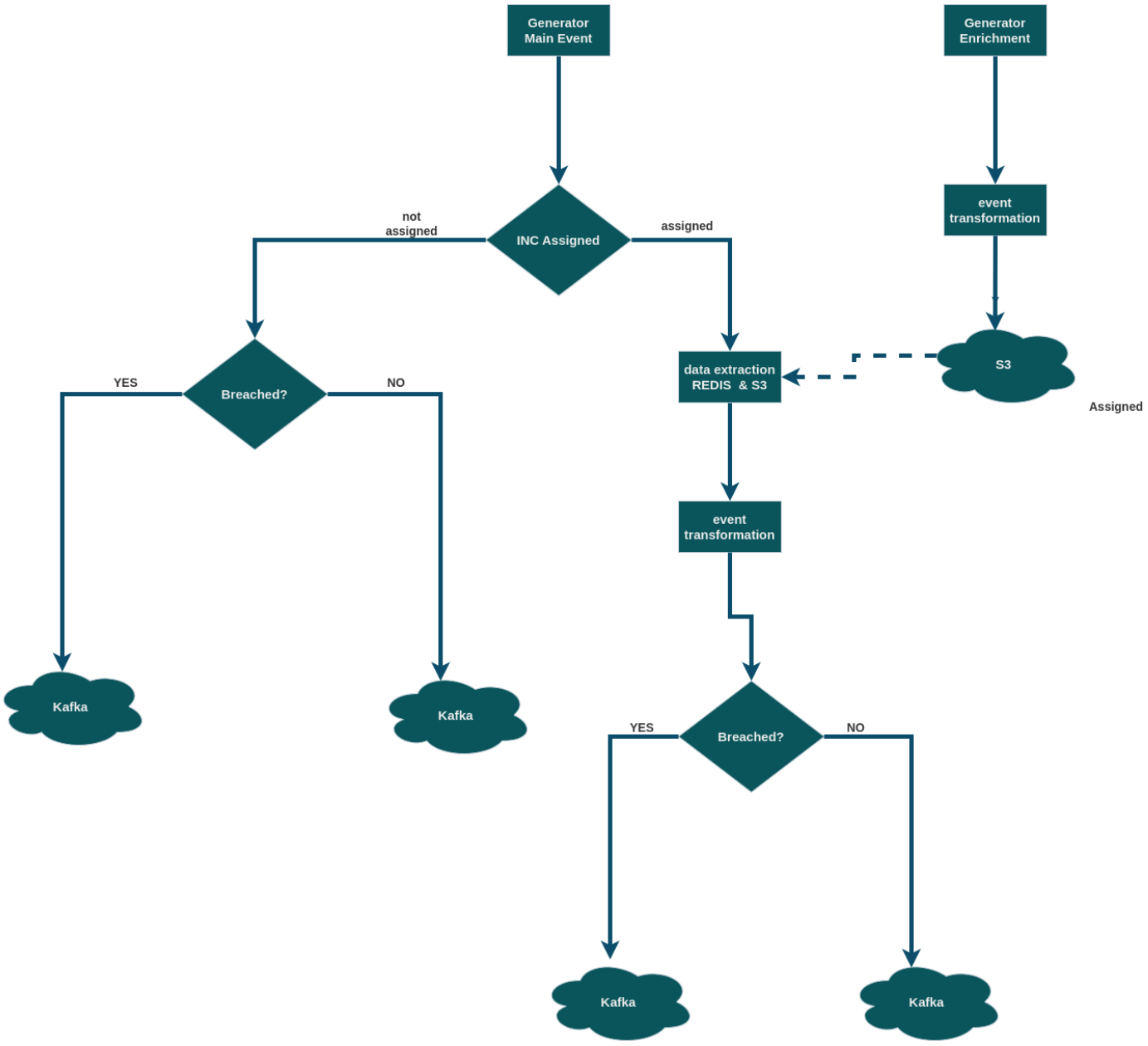
Example: Zadanie 3 - INC Handling

INC Handling (ING)

Main Flow

- Segregacja incydentów na grupy:
  - assignment (YES / NO)
  - Breached (YES / NO)
- Wyliczanie czy INC breached:
  - High: 2H
  - Medium: 3D
  - Low: 5D
- Flow wynikowe powinno być wysłane na Kafkę na topic
  - **incReportingBreachedAssigned,**
  - **incReportingBreachedNonAssigned,**
  - **incReportingNonBreachedAssigned,**
  - **incReportingNonBreachedNonAssigned**

Data flow model:



INC list

```
[{
    "Status" : "New",
    "Severity" : "High",
    "Assignee" : "",
    "Team" : "ITSecurity",
    "IncydentTitle" : "EICAR virus filetest found",
    "IncidentMessage" : "EICAR virus filetest found",
    "IncidentNumber" : "000001",
    "Cloud" : "Azure",
    "Timestamp" : "1704658670579"
},
{
    "Status" : "Active",
    "Severity" : "Medium",
```

```
    "Assignee" : "AA22BB",
    "Team" : "ITSecurity",
    "IncydentTitle" : "File without the ownet found",
    "IncidentMessage" : "File without the ownet found. Please remove or
chage the owner",
    "IncidentNumber" : "000002",
    "Cloud" : "AWS",
    "Timestamp" : "1704658685441"
},
{
    "Status" : "Active",
    "Severity" : "Low",
    "Assignee" : "AA33BB",
    "Team" : "ITSecurity",
    "IncydentTitle" : "Old java package found",
    "IncidentMessage" : "Old java package found - please upgrade",
    "IncidentNumber" : "000003",
    "Cloud" : "GCP",
    "Timestamp" : "1704659596141"
},
{
    "Status" : "Closed",
    "Severity" : "High",
    "Assignee" : "AA11BB",
    "Team" : "ITSecurity",
    "IncydentTitle" : "EICAR virus filetest found",
    "IncidentMessage" : "EICAR virus filetest found",
    "IncidentNumber" : "000004",
    "Cloud" : "GCP",
    "Timestamp" : "1704659730274"
},
{
    "Status" : "New",
    "Severity" : "High",
    "Assignee" : "",
    "Team" : "ITSecurity",
    "IncydentTitle" : "Many log in attempts found",
    "IncidentMessage" : "Many log in attempts found for user AA66BB",
    "IncidentNumber" : "000005",
    "Cloud" : "GCP",
    "Timestamp" : "1704659730274"
}
]
```

S3 - personal database


```
[
{
    "Name" : "Kamil",
    "Surname" : "Kowalski",
    "Email" : "Kamil.Kowalski@example.com",
    "EmployeeIdNumber" : "AA11BB",
    "Department" : "ITSecurity",
    "Position" : "Engineer"
},
{
    "Name" : "Marta",
    "Surname" : "Nowak",
    "Email" : "Marta.Nowak@example.com",
    "EmployeeIdNumber" : "AA22BB",
    "Department" : "ITSecurity",
    "Position" : "Expert"
},
{
    "Name" : "Marcin",
    "Surname" : "Osoba",
    "Email" : "Marcin.Osoba@example.com",
    "EmployeeIdNumber" : "AA33BB",
    "Department" : "ITSecurity",
    "Position" : "Trainee"
},
{
    "Name" : "Kamila",
    "Surname" : "Nowacka",
    "Email" : "Kamila.Nowacka@example.com",
    "EmployeeIdNumber" : "AA44BB",
    "Department" : "ITSecurity",
    "Position" : "Engineer"
}
]
```


END Event


```
{
  "IncydentTitle" : "EICAR virus filetest found",
  "AssigneePosition" : "Engineer",
  "Team" : "ITSecurity",
  "AssigneeEmail" : "Kamil.Kowalski@example.com",
```

```
  "AssigneeDepartment" : "ITSecurity",
  "AssigneeName" : "Kamil",
  "AssigneeSurname" : "Kowalski",
  "Cloud" : "GCP",
  "Breached" : "YES",
  "Status" : "Closed",
  "IncidentNumber" : "000004",
  "IncidentMessage" : "EICAR virus filetest found",
  "AssigneeEmployeeIdNumber" : "AA11BB",
  "Severity" : "High",
  "Timestamp" : "1704659730274"
}
```


Flow Configuration File:

INC_handling.json