Data Flow Description

# Revision:

|  |  |  |  |
| --- | --- | --- | --- |
| Author | Description | Version | Date |
| Kim Hoang Ngoc | Add this document | 1.0 | 04/12/2010 |
| Kim Hoang Ngoc | Modify data structure | 1.1 | 06/12/2010 |

# ID

# Name

**Normalized Alert.**

# Description

This data is gotten from the Alert Database in order to make Attack Graph.

# Source

Alert Database

# Destination

Aggregate Alert

# Type of Data Flow

File Screen Report Form Internal

# Data Structure Traveling with the Flow

Normalized Alert = Alert + Heartbeat

Alert = Analyser + CreateTime + DetectTime + AnalyserTime + Source + Target + Classification + Assessment + AdditionalData

Analyser = AnalyserID + Name + Manufacturer + Model + Version + Class + OSType + OSVersion.

Source = Node + User + Process + Service

Target = Node + User + Process + Service + FileList

Heartbeat = Analyser + CreateTime + AdditionalData

# Volume/Time

1-10/ms

# Comments

# Unresolved Issue