Data Flow Description

# Revision:

|  |  |  |  |
| --- | --- | --- | --- |
| Author | Description | Version | Date |
| Kim Hoang Ngoc | Add this document | 1.0 | 04/12/2010 |

# 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 Type +  
 Begin Time +  
 End Time +  
 Source IP +  
 Destination IP +  
 Source Port +  
 Dest Port.

# Volume/Time

# Comments

# Unresolved Issue