Data Flow Description

# Revision:

|  |  |  |  |
| --- | --- | --- | --- |
| Author | Description | Version | Date |
| Kim Hoang Ngoc | Add this document | 1.0 | 24/12/2010 |

# ID

# Name

**Hyper Alert.**

# Description

Normalized Alerts are aggregated into Hyper Alerts. This data is then used to make Raw Attack Graph.

# Source

Aggregate Alert

# Destination

Correlate Hyper Alert

# Type of Data Flow

File Screen Report Form Internal

# Data Structure Traveling with the Flow

Hyper Alert = Real Fact + Hypert Alert Type Name + BeginTime + EndTime.

Real Fact = Fact Name + Fact Value.

Fact Name = Name.

Fact Value = [IP address, Port].

Hyper Alert Type Name = Name.

# Volume/Time

1-10/ms

# Comments

# Unresolved Issue