Data Flow Description

# Revision:

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

# ID

# Name

**Knowledgebase Data**

# Description

This data is the backbone of the program. It is used to aggregate alert as well as construct attack graph.

# Source

Knowledgebase Database

# Destination

Correlate Hyper Alert

# Type of Data Flow

File Screen Report Form Internal

# Data Structure Traveling with the Flow

KnowledgeBase Data = {Predicate} +  
 {Implication} +  
 {Hyper Alert Type}.

Predicate = Name +  
 {Argument}.

Argument = ID +  
 Position +  
 Type.

Implication = Implying Name +  
 Implied Name +  
 {Argument Map}.

Implying Name = Name.

Implied Name = Name.

Argument Map = Implying Argument ID +  
 Implied Argument ID.

Hyper Alert Type = Name +  
 {Fact} +  
 Protocol +  
 Prerequisite +  
 Consequence.

Fact = Name +  
 Type.

Protocol = Name.

Prerequisite = {Predicate}.

Consequence = {Predicate}.

# Volume/Time

# Comments

# Unresolved Issue