Data Flow Description

# Revision:

|  |  |  |  |
| --- | --- | --- | --- |
| Author | Description | Version | Date |
| Thi Nguyen Tran | Add this document | 1.0 | 05/12/2010 |

# ID

**5.1**

# Name

**Knowledgebase Data**

# Description

Necessary information to build attack graph from alerts and raise alert to system administrator.

# Source

Process P5

# Destination

Data Store D1. Knowledgebase

# Type of Data Flow

File Screen Report Form Internal

# Data Structure Traveling with the Flow

Knowledgebase Data = {Predicate} +

{Implication} +

{Hyper Alert Type}

Predicate = Predicate Name +

{Argument}

Argument = Argument ID +

Argument Position +

Argument Type

Implication = Implying Name +

Implied Name +

{Arguments Map}

Arguments Map = Implying Argument ID +

Implied Argument ID

Hyper Alert Type = Hyper Alert Type Name +

{Fact} +

{Protocol} +

Prerequisite +

Consequence

Fact = Fact Name +

Fact Type

Protocol = Protocol Name

Prerequisite = {Predicate}

Consequence = {Predicate}

# Volume/Time

# Comments

# Unresolved Issue