Data Dictionary

# Description:

This document includes:

* Data structures for *D. AttackGraphDatabase* data store.
* Process specifications for *3. Make Graph* process and its sub processes.
* Data flows used for process 3 and its sub processes.

# Revision:

|  |  |  |  |
| --- | --- | --- | --- |
| Author | Description | Version | Date |
| Kim Hoang Ngoc | Add this document | 1.0 | 23/11/2010 |

# Content

## D.AttackGraphDatabase

//Written later

# Data Flows

Normalized alerts are from Alert Database.

Hyper Alert (base on Hyper Alert definition in PS\_Process5\_AddKnowledge)

= Name +

{Fact} +

Protocol +

Prerequisite +

Consequence

KnowledgeBase Data are from KnowledgeBase database.

Raw Attack Graph //Written later

Config is the data which guides the program to show the graph to Admin.

# Process specification

Normalized alerts from Alert Database are aggregated to Hyper Alert.

Hyper Alerts are correlated to make Raw Attack Graph (attack scenario) with the Knowledgebase Data.

Raw Attack Graph is stored in the Attack Graph Database.

Raw Attack Graph is adjusted base on the config of Admin to make Attack Graph which is sent to Admin.