Process Specification

# Revision:

|  |  |  |  |
| --- | --- | --- | --- |
| Author | Description | Version | Date |
| Kim Hoang Ngoc | Add this document | 1.0 | 28/11/2010 |
| Kim Hoang Ngoc | Modify Process Logic | 1.1 | 01/12/2010 |

# Number: 3

# Name: Make Graph

# Description: This process get the alerts from the database to make Attack Graph for Admin.

# Input Data Flow:

Normalized alerts are from Alert Database.

KnowledgeBase Data are from KnowledgeBase database.

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

# Output Data Flow:

Attack Graph //written later

# Type of Process:

Online Batch Manual

# Subprogram/Function Name:

3.1 Aggregate Alert

3.2 Correlate Hyper Alert

3.3 Process Graph

# Process Logic:

DO aggregate Normalized Alert.

DO correlate Hyper Alert.

DO store Raw Attack Graph to Attack Graph Database.

DO get Raw Attack Graph from Attack Graph Database.

DO process Raw Attack Graph.

# Unresolved Issues:

How to store the Raw Attack Graph in the database.