Process Specification

# Revision:

|  |  |  |  |
| --- | --- | --- | --- |
| Author | Description | Version | Date |
| Kim Hoang Ngoc | Add this document | 1.0 | 28/11/2010 |

# 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:

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.

# Unresolved Issues:

How to store the Raw Attack Graph in the database.