

USER GUIDE



Predictive Analytics Engine (PAE)

Document reference: QSL-PAE-1/11 Issue: 1.1 January 2011

Quantar Solutions Ltd. - Cambridge - United Kingdom - www.quantarsolutions.com

This document was written by Quantar Solutions Ltd.
Copyright © Quantar Solutions Ltd. 2011.

CONTENTS

1. Introduction.....	Page 3
2. Configuration.....	Page 4
3. Risk Files.....	Page 7
4. Risk Results	Page 8
5. Attack Data.....	Page 10
6. Risk Trends.....	Page 11
7. Run Model.....	Page 12
8. Glossary of Terms.....	Page 14

INTRODUCTION

PAE Multi-Model Approach

Network operational risks are those associated with virus attacks, targeted attacks (hacking) and physical attacks (damaging or immobilizing technology infrastructure).

Using quantitative modelling techniques within PAE enables a quantification of risk metrics for such attacks.

PAE provides greater stochastic modelling capabilities than within n-ORM and are able to compute a wider range of analytical measures aimed at meeting new and emerging regulatory requirements relating to stress testing of risk models.

The system comprises a primary three-phase approach to modelling, with these being a time-series component and a post-processing layer.

Within phase one, there are a number of optional features that may be enabled or disabled by the end user, these being:

- linear or exponential process model;
- normal or weighted data model;
- standard L-S or robust model.

Within the second phase, a Monte-Carlo simulation module is utilized, which takes a range of input and configuration data and computes risk distributions.

The calculation engine generates probability functions, enabling various statistical outputs to be drawn and utilized within overall risk management and business continuity programs.

Once configured, PAE will then run at start-up in the language assigned. Using this capability can be useful for multi-geography; multi-language organizations.

PAE Start-up

Launching PAE initiates the login screen. PAE is delivered with the default settings of:

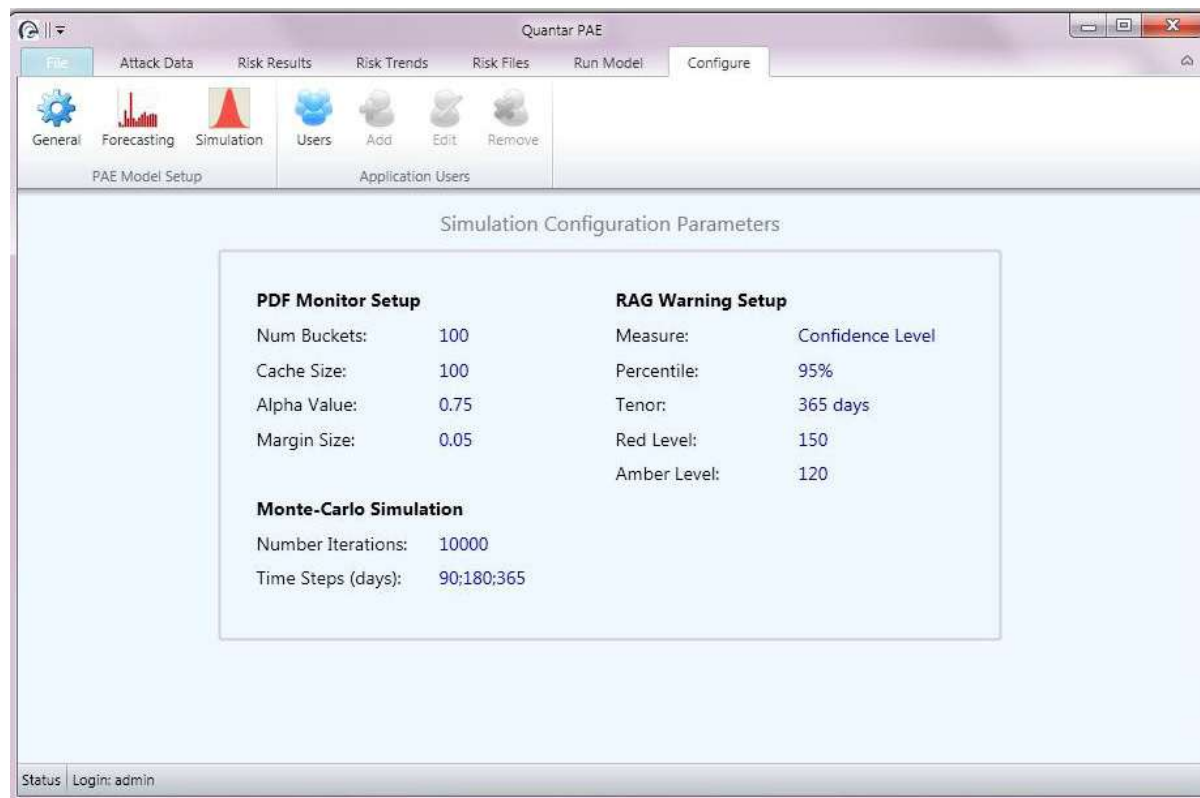
User ID: admin

Password: quantar

Once logged in, the Change Password Filed is then available for establishing a secure and individual-specific password.

Configure

Select "Configure" in the main tabs and the following screen is visible:



Simulation

This summary screen gives the user the default parameters within the PAE "Simulation" system that can be configured according to requirements by users with "Administrator" power.

The Probability Distribution Function (PDF) Monitor Setup indicates the number of buckets utilized in the data set monitoring and the cache size. These parameters should only be altered by those with a strong understanding of the statistical impact of altering the bucket number.

The Monte-Carlo Simulation parameter settings display the number of iterations run for a given data set. The default setting is set at 10 000 iterations. This should be regarded as the minimum acceptable level and should therefore not be reduced below this value.

Increasing the number of iterations will increase the processing time required by PAE to arrive at the simulation values display. The performance of the machine upon which PAE is installed is therefore a consideration of the number of iterations a user may wish the default number to be set at.

RAG Warning Setup

The RAG warning system comprises the red./ amber / green coloured warning icons within the PAE main display and are the means by which users may be alerted to acceptable risk thresholds being breached or about to be breached. The default should always result in a Green status symbol being displayed.

The Confidence level default is set at 95% over a period of 365 days. Changes to these parameters should be carefully considered. Altering the tenor from 365 may be required by organizations seeking to understand the PDF for a shorter period, for example per quarter or half-year. A higher than 95% confidence level may be required in certain circumstances. The Amber and Red parameters should reflect the risk appetite of the organization concerned.

Forecasting

The Forecasting Configuration Parameters are displayed for both the Attack Forecasting Model and the Infection Forecasting Model.

For each case, the user is able to configure for the extrapolation model, the fitting of the model to the data, the weighting required for the model and the weight parameters.

The default settings are
Extrapolation = Linear
Fitting = Least-Squares
Weighting = Normal
Weight Parameters = 0

Users

Selecting the "Users" button displays the profile of the users currently within PAE. They are listed by User ID; Type; the date that user was added to the system, and a description.

Using the "Add" button – this generates a screen enabling the administrator to add a users and to define specific fields of a User ID; a Password; Privilege level for the new user; a descriptive details where required.

NOTE: User ID's and passwords cannot be shorter than 5 characters long for reasons of security

Using the "Edit" button – this enables user profiles, passwords, privilege level and the description of a user to be changed and such changes saved.

Using the "Delete" button – this enables users to be deleted completely from the system. Select the user to be deleted from the system and then click on the "Delete" button. The administrator will be requested to confirm the deletion before this takes effect.

General

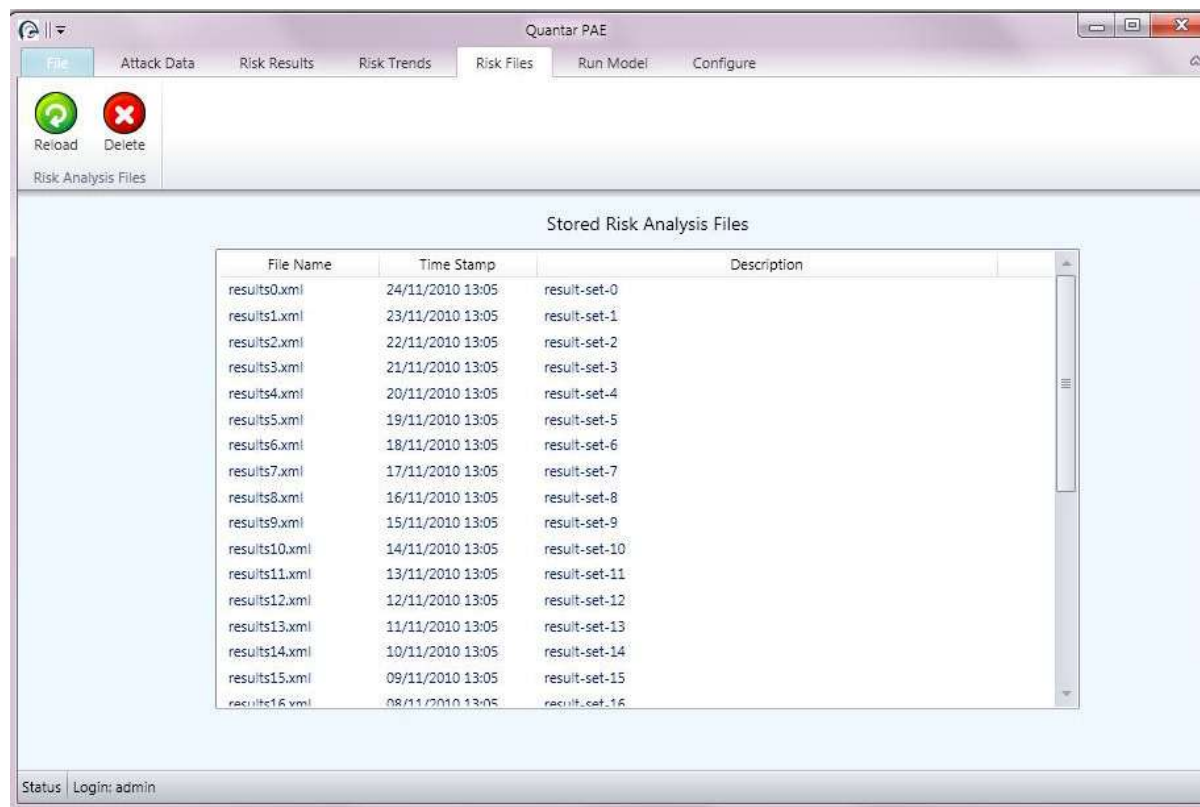
Selecting the "General" button will display the location of the application data on the computer upon which PAE is installed. The system will start upon launch in the default language set by the system administrator and the default language is displayed here.

NOTE: The currency setting is set for display purposes only. There is no default currency from which PAE extrapolates a currency exchange.

The Risk Hierarchy – display the order in which the system displays either the severity or the threat. The default is set at severity/threat_id and should only be changed where analysis of particular attack types is desired.

Risk Files

Selecting the "Risk Files" tab will lead to the following screen:



This displays the stored risk analysis files and their name, datestamp created by the IPTAP back-end system, a results set label and a description field.

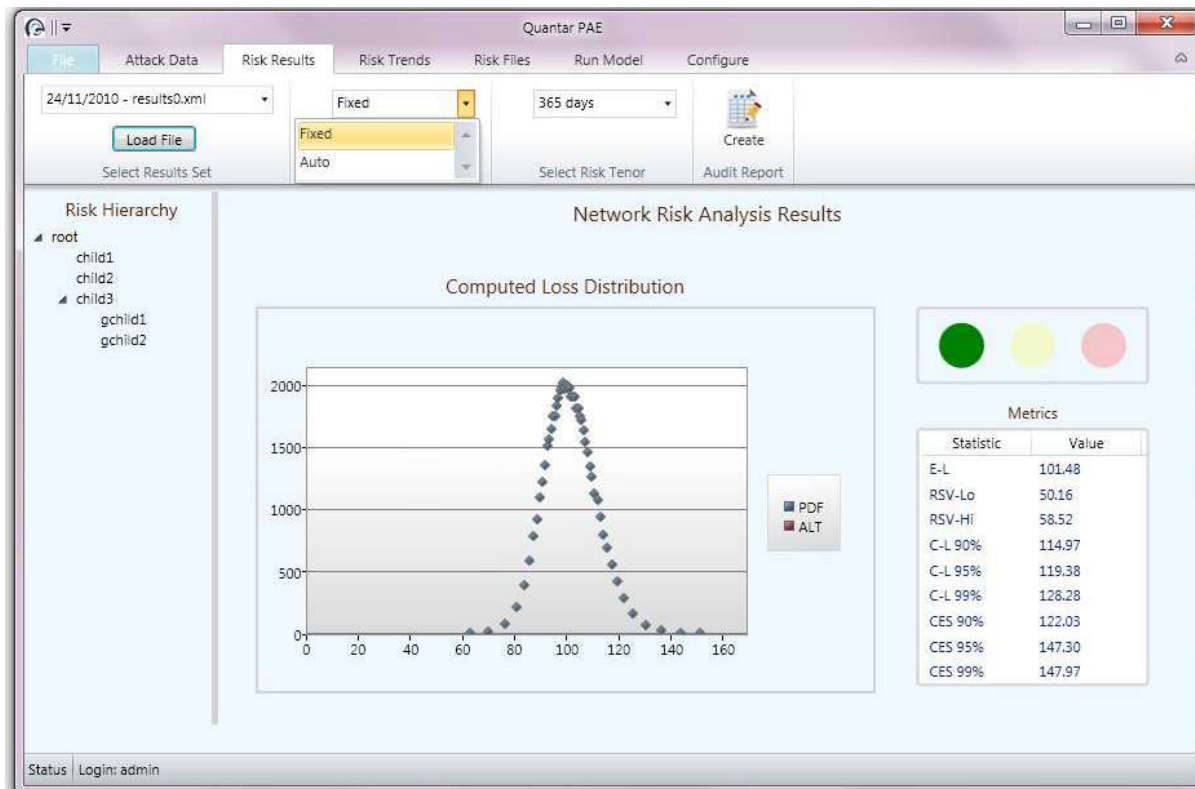
The files can be reloaded into the PAE system by clicking the "Reload" button.

It is also possible to view the risk analysis files from within the drop-down menu within the "Risk Results" section of the application.

If a data set should be removed to avoid possible incorrect selection, it may be deleted by highlighting the relevant data set and selecting the "Delete" button. The user will be prompted to confirm the deletion by the system.

Risk Results

Selecting the “Risk Results” tab will display the following screen:



The “Computed Loss Distribution” for a given set of data is displayed as a probability distribution function (PDF) for a given period.

Selecting the required data set is achieved by selecting the relevant file from the “Load File” functionality.

The “Plot Scale” allows the user to select from a fixed scale or an automatic one.

The “Risk Tenor” is configured for the period required at 90 days; 180 days; 365 days.

It is possible to “drill-down” into the PDF and reviewing the impact by selecting a path through the “Risk Hierarchy”. Selection is by highlighting the child/grandchild level within the results hierarchy and the PDF will alter as the hierarchy is scrolled through.

The RAG (red; amber; green) functionality can be clearly seen, with the example displaying a green status.

The table below the RAG warning panel displays the results of the "Network Risk Analysis". The metrics are displayed according to the statistic and value generated by PAE (refer to Glossary for abbreviations).

Selecting the "Create Audit Report" spawns a pop-up window displaying the results table and the relevant date. This report may be printed or saved as either an .xls file or a .pdf file for audit and compliance purposes where required.



PAE Network Risk Audit Report

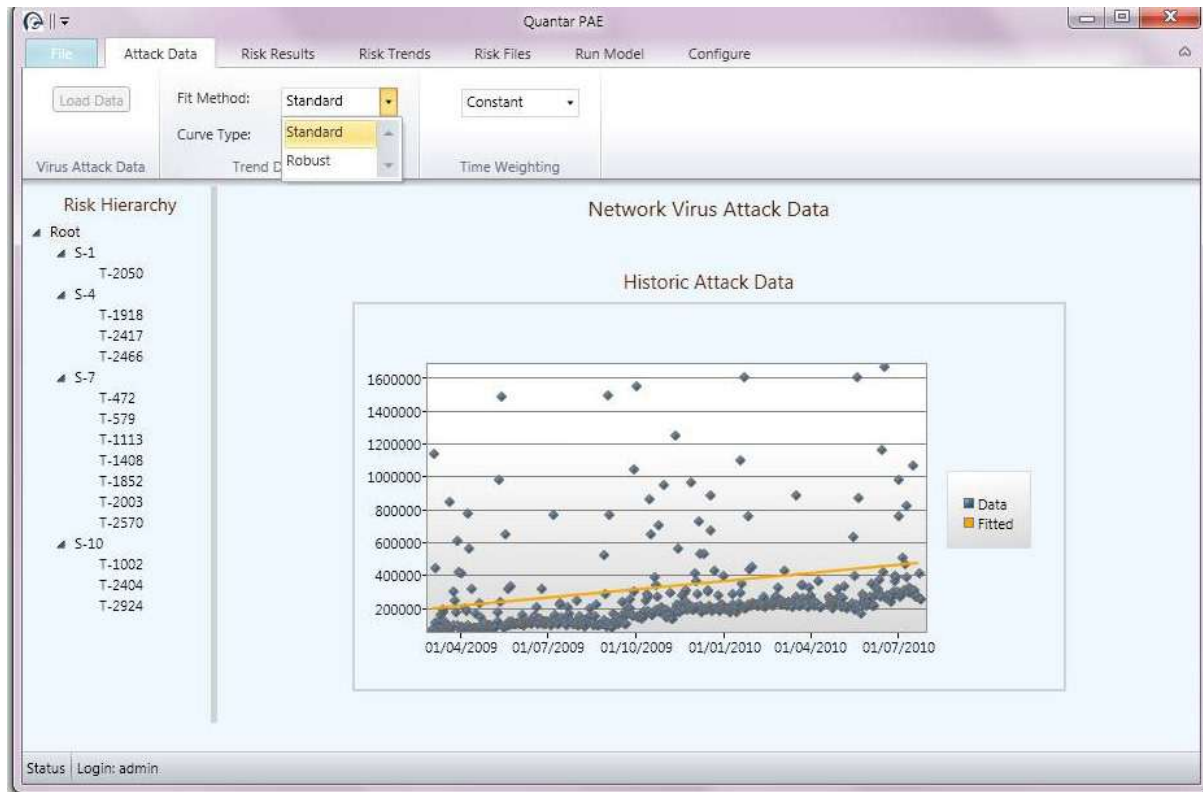
24-November-2010

RAG Risk Value: 119.38 GBP

Risk Measure	Value
E-L	101.48
RSV-Lo	50.16
RSV-Hi	58.52
C-L 90%	114.97
C-L 95%	119.38
C-L 99%	128.28
CES 90%	122.03
CES 95%	147.30
CES 99%	147.97

Attack Data

Selecting the "Attack Data" tab displays the following screen



After selecting the data file from within the "Risk Files" section of the application and loading it, PAE displays the related Historic Risk Data in a hierarchical manner.

At the root of the risk hierarchy, the user is able to toggle through the results of the historic attack data and review the impact upon the distribution over a specified time period.

The "Trend Data Fitting" function allows the user to determine whether a "Robust" or "Standard" fit to the attack data should be used in the analysis. The curve to be fitted to the attack data can be changed from a "Linear" to an "Exponential" fit.

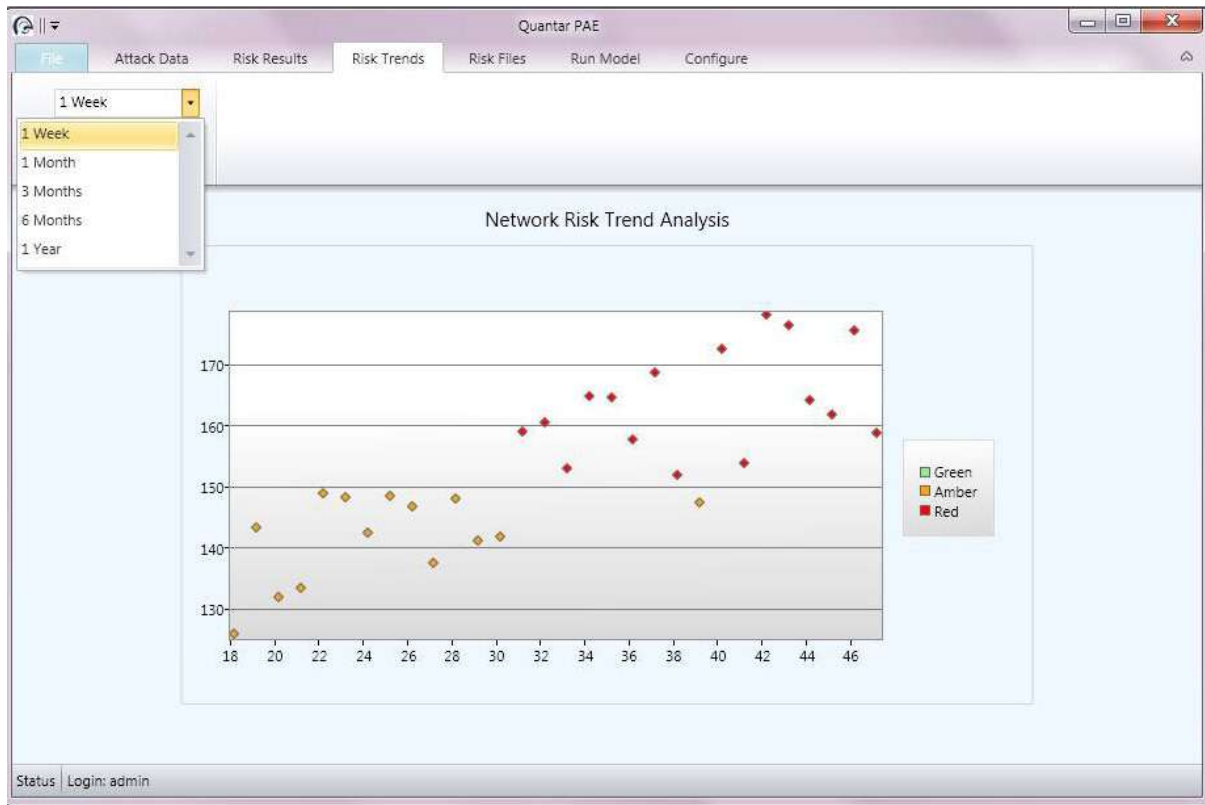
The final user defined parameter for the Historic Attack Data is the "Time Weighting". The user can select from a Constant; 365; 180; 90; and 30 day weighting attached to the Historic Attack Data.

The display indicates both the actual attack data experienced by the network, indicated by the dark grey plots over a given time period, plus the fit of the attack data trend by the yellow line.

The fit of the trend is determined according to the parameters selected by the user, as outlined above.

Network Risk Trends

Selecting the "Risk Trends" tab displays the following screen

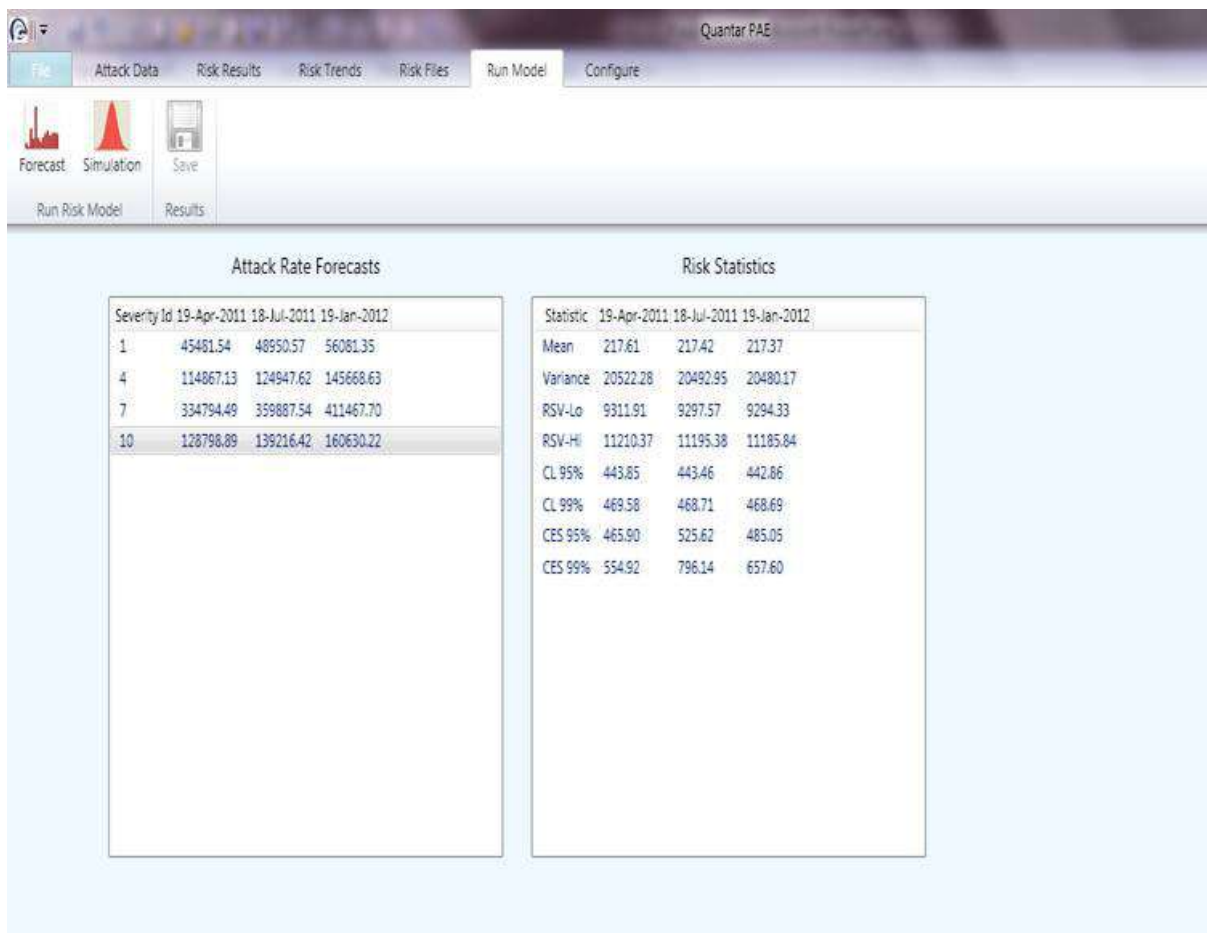


This displays in a clear and concise manner the actual risk trend for the network of the user-organization over a given period.

The RAG warning plot is shown and the Trend Interval offers the user the option of selecting between 1 week; 1 month; 3 months; 6 months; and a year of network risk trend analysis.

Run Model

Selecting the "Run Model" tab displays the following screen



Here the results of the Attack Rate Forecast and the Risk Statistics are displayed.

For the Attack Rate Forecast, the display lists firstly the Severity ID of the types of attack followed by the number of attacks for that type of Severity ID over a given period.

For the Risk Statistics, the display lists firstly the Statistic, followed by the values of each statistic over a given time period that corresponds with the Attack Rate Forecast periods. **NOTE** for abbreviations, refer to the Glossary of Terms.

By selecting the Severity ID of the Attack Rate Forecast required, the user may then select the "Simulation" button and PAE will then run the model to determine the Risk Statistics for a given Severity ID.

The Confidence Level (CL) and Conditional Expected Shortfall (CES) are usually the most relevant values for managing network operational risks. Additional data displayed should be used by those with sufficient statistical knowledge to make their applicability to the overall risk exposure worthwhile.

Output results from running the model can be saved to a file by selecting the "Results" – "Save" button.

GLOSSARY OF TERMS

Alt – Alternative view of the probability in the tail on a log-scale **NOTE:** Function disabled in all versions until unlocked by Quantar System Administration

CL – Confidence Level - (for the percentage level of X)

E-L – Expected Loss

CES –Conditional Expected Shortfall – this is the expected loss if the loss exceeds the given confidence level of loss. The CES should always be greater than the associated confidence level, that is, the amount by which it more reflects how “fat” the tail of the distribution is. The CES is therefore a better measure of risk than the confidence level.

Hierarchy – this function enables data to be tagged. The risk profile can then be viewed at an aggregate level. It may also be viewed as a sub-set of the data e.g. broken down according to the severity”

PDF- Probability Distribution Function – this is the probability density

Risk Trends X-Axis - this is the number of days that have elapsed since the first stored data set

Risk Trends Y-Axis – this is the risk measure and is the primary measure used by PAE according to the configuration set by the user.

RSV-Lo / Hi: Root Semi Variance Lo / Hi – this is akin to the standard deviation but differs in that it is computed separately for the upper and lower parts of the loss distribution. As a consequence, where there is skewed distribution which is “fatter” on the high side than the low side, then the figure for the “Hi” number will be greater than the “Lo” number. If the “Hi” and “Lo” figures are the same, then the distribution will be symmetrical.

X-Axis – this is the computed loss measure

Y-Axis – this is the probability density (or the proportion)

