

PTA Professional Edition Reports

System's Status

Provides a "bottom lines monitor" of the threat model project with an updated view of the **Risk Status** of the system, as well as indications regarding the progress of the threat analysis process.

The **Total Value of Assets**, **Total Cost of Countermeasures** and the amount of money that is **Already Invested in Mitigation** provides the important financial figures.

Top Current Risk Threats is a bar chart presentation of the current top 5 risky threats. The risk values are displayed in \$. The names of the threats are displayed in the details table below the bar chart.

Risk History is a graph which displays the levels of risk in the system along the time axis of the threat analysis process. The levels of various risks are presented in percentage of the total value of system assets.

Analysis History is a graph that displays the numbers of vulnerabilities, threats and countermeasures defined in the model along the time axis of the threat analysis process.

Countermeasures Theoretical Cost-Effectiveness

This analysis report produces a list of countermeasures sorted by their **Theoretical Cost-Effectiveness** that is based on the assumption that all countermeasures will be implemented. The theoretical cost-effectiveness of a countermeasure is given in % of system's risk mitigated by the countermeasure divided by the cost of the implementation of the specific countermeasure.

Since implementing all countermeasures is, in most cases, not practical, it is recommended to complement the results of this report with the "**Optimized Risk Reduction Plan**" analysis report.

For each countermeasure, the report displays calculative parameters as follows:

- **Cost-Effectiveness**
- **Implementation Cost**
- **Overall Mitigation**

In addition, the report displays a list of threats for which a specific countermeasure is included in their mitigation set.

Mitigation Plans by ROSI

This analysis produces a list of mitigation plans for threats sorted in a descending order by their **ROSI** value. **ROSI (Return On Security Investment)** is a very common quantitative criterion for comparing security solutions. To determine the return on security investment we simply subtract the annual cost of the security mitigation solution from what we expect to lose in a year and present the result in percents.

The following calculative values are displayed for each of the mitigation sets in the report:

- **Mitigation Plan ID** is a comma separated concatenation of the Countermeasures IDs of all countermeasures included in the mitigation plan.
- **VAR Mitigated by Mitigation Plan** is the value of assets under risk which is mitigated by the mitigation plan.
- **Cost of Implementing Mitigation Plan** is the cost per year of implementing all countermeasures in the mitigation plan calculated by summing all countermeasures' weighted costs.
- **ROSI** - Return On Security Investment is defined by the following formula:

$$\text{ROSI} = \frac{(\sum \text{Value at Risk} * (\text{Mitigation Level}/100)) - \text{Mitigation Cost}}{\text{Mitigation Cost}} * 100$$

\sum - summation over all threats mitigated by the specific mitigation plan

Value at Risk (AKA Risk Exposure or ALE - Annual Loss Expectancy) is the threat's damage multiplied by the threat's probability which expresses the number of times the threat will materialize per year (ARO).

Mitigation Level is the estimated level (in percents) of mitigation that the threat's mitigation plan provides.

Mitigation Cost is the cost per year of implementing all countermeasures in the mitigation plan.

- **Threats Mitigated by Mitigation Plan** is a list of all threats which are mitigated by a specific mitigation plan. For each threat in the list the following fields are displayed: Value at Risk (AKA Risk Exposure or ALE - Annual Loss Expectancy) which is the Threat's Maximal Risk and Mitigation Level which is the Threat's Maximal Mitigation. In addition the threats list includes the Mitigation Set which is a comma separated concatenation of the IDs of the actual countermeasures which mitigate the specific threat (and might be a subset of the mitigation plan analyzed).
- **Countermeasures in Mitigation Plan** is the list of all countermeasures included in the specific mitigation plan. For each countermeasure in the list, the report displays the Cost which is the specific countermeasure's weighted cost

Note: negative ROSI values imply that the investment in the countermeasures is not well justified from a financial point of view.

Optimized Risk Reduction Plan

This analysis report produces a recommended sequence of mitigation steps that will reduce the system's risk to a given target level in the most cost-effective way. Each step in the proposed risk reduction plan is comprised of countermeasures that should be implemented in order to achieve the step's contribution to risk reduction.

Notes:

1. The optimization mechanism starts from the current status of countermeasures implementation - countermeasures marked as 'already implemented' will not be assigned to the proposed risk reduction plan. The processing may take several minutes for systems with large number of entities.
2. If the implementation cost of a countermeasure is not specified, the default cost value is determined as 1\$.
3. The target risk level should be between the system's maximal risk and the system's minimal risk levels.
4. All countermeasures in a given step should be implemented in order to achieve the step's contribution to risk reduction.
5. The contribution of each step in the plan to risk reduction is accurate only if all steps preceding it are implemented. Therefore, in order to achieve the target risk level, all countermeasures in the outcome sequence should be implemented. In case of partial implementation, the optimization should be run again in order to create an updated sequence that reflects the current system status.

The System's Risk Status section of this report contains the following fields:

- **Maximal Risk Level**
- **Current Risk Level**
- **Minimal Risk Level**

For each of the steps in the optimized sequence the report displays a list of countermeasures that should be implemented in the specific step. For each of the countermeasures in a specific step the following information is displayed costs values:

- **Countermeasure Implementation** is a specific countermeasure's weighted cost
- **Accumulated per Step** is the sum of all countermeasure implementation costs preceding the specific countermeasure in the step.
- **Accumulated per Plan** is the sum of all countermeasure implementation costs preceding the specific countermeasure in the proposed optimized risk reduction plan.

At the end of a step countermeasures list, the report displays the **Remaining Risk** which is the system's current risk that remains after implementation of the specific step's countermeasures.

Detailed Threats

This report produces a list of all the system's threats, ordered by their **Current Risk Level**. It shows the following parameters for each threat:

- **Probability**
- **Damage**
- **Maximal Risk**
- **Minimal Risk**
- **Current Risk**
- **Maximal Mitigation Available**

In addition, the report displays lists of all model entities associated with each threat and the relevant calculative parameters as follows:

- **Threaten Assets** is a list of all assets threatened by the threat and the Level of Damage which is the Threat's Damage Level to Asset for each of the threatened assets.
- **Exploited Vulnerabilities** is a list of all vulnerabilities exploited by the specific threat.
- **Recommended Countermeasures** is a list of all countermeasures that might take part in the threat's mitigation plan. The Included In Mitigation Set check sign indicates whether or not the countermeasure is actually included in the mitigation plan.
- **Entry Points** is a list of entry points exploited by the attacker to materialize the threat scenario.
- **Attacker Types** is a list of attacker types that might initiate the threat's attack.
- **Tag** is a list of tags associated with the threat.

Detailed Assets

This report produces a detailed list of all assets ordered by their annual weighted value. The following fields are displayed for each asset:

- **Weighted Value in \$**
- **Weighted Value in %**
- **Maximal Risk**
- **Current Risk**
- **Minimal Risk**

In addition, the report displays the following lists of entities associated with each asset as follows:

- **Threatening Threats** is a list of threats that threaten a specific asset. For each threat in the list, the report displays the Level of Damage which is the Threat's Damage Level to Asset and the Probability which is the Threat's Probability.
- **Tags** is a list of tags associated with the specific asset.

Detailed Vulnerabilities

This report produces a detailed list of all vulnerabilities in the threat model ordered by their IDs.

In addition, the report displays the following lists of entities associated with each vulnerability:

- **Exploiting Threats** is a list of threats which exploit the specific vulnerability.
- **Mitigating Countermeasures** is a list of countermeasures which mitigate the specific vulnerability.
- **Tags** is a list of tags associated with the specific asset.

Top Threats by Current Risk

This report produces a chart of top risky threats, ordered by their **Current Risk Level**.

The threats' names and their risk values in \$ are displayed above the chart.

Note:

For an updated list of PTA reports please visit: <http://www.ptatechnologies.com/ptareports.htm>

© PTA Technologies 2005 - 2008

www.ptatechnologies.com

+972 3 5443085