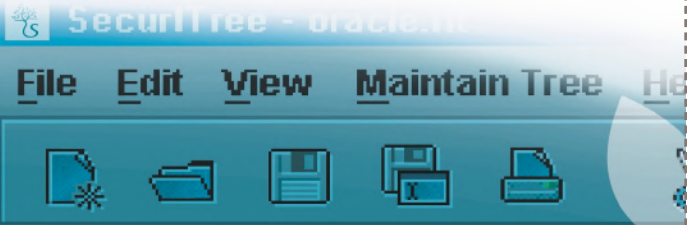




Amenaza
TECHNOLOGIES LIMITED



Dare You Risk IT?

SecurITree will help you decide!

Exploit App Defects



SecurITree

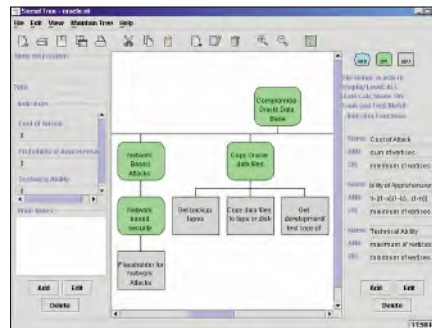
The first graphical risk analysis package of its kind

Information technology risk is a fact of life in today's interconnected business world.

Many companies strive to “minimize” risk. This goal is incorrect because it leads to a reduction in profit and results in lost opportunities. A more enlightened approach is to “optimize” risk.

Optimizing risk accepts the fact that all profitable business ventures involve some risk. An optimal level of risk is one which maximizes profits over the long haul, i.e., it accepts the notion that occasional managed incidents of limited impact are a necessary evil in the course of business activities. Companies then benefit the most by spending their information technology (IT) security dollars to eliminate unnecessary and excessive risk.

Amenaza Technologies has created the first commercially available threat tree-based risk assessment tool and methodology specifically designed to identify which IT risks need to be mitigated.



Screenshot of SecurITree

SecurITree is a strategic solution which allows you to analyze and understand the risks in your IT systems. Unlike most security tools (firewalls, VPNs, intrusion detection systems) which address tactical security issues, SecurITree analyzes the design of systems, before or after implementation.

EMPLOYING A SOPHISTICATED MODELING TECHNIQUE called “threat tree analysis”, SecurITree provides a graphical way for the IT professional to understand IT risk. The steps of the methodology:

- Model an IT system’s vulnerabilities graphically in a tree-based representation
- Identify people and events (threat agents) hostile to an IT system
- Mathematically compare the capabilities of threat agents to the weaknesses of an IT system
- Reveal the weaknesses most likely to be exploited in an IT system
- Eliminate threats which are unlikely to be exploited by the threat agents
- Prioritize remaining threats which represent potential areas of concern
- Support decision making and the creation of an IT security action plan intuitive for both technical experts and management alike

SecurITree’s systematic, graphical tree-based approach allows you to determine which threats are most likely to occur. By pruning tree nodes that your enemies are incapable of achieving, you know which threats are of no practical importance. The remaining leaves are then evaluated to determine whether the risk is tolerable or requires mitigation procedures.

SecurITree helps to determine an optimal level of risk. Companies benefit by deploying their IT security resources to eliminate unnecessary and excessive risk.

Dare You Risk IT?

Discover the answers with SecurITree



Compromise
Oracle

Copy
data files

Get backup
tapes

Copy data
to tape

Get
test data



Contact Us

406-917 85 St SW, Ste 125
Calgary, AB Canada T3H 5Z9

TEL (403) 263-7737

FAX (403) 278-8437

TOLL-FREE 1-888-949-9797

E-MAIL info@amenaza.com

WEB www.amenaza.com

Grow Your Own Tree

Secur/Tree allows you to create threat tree models of your information systems quickly and easily. The threat trees match your system design or implementation, not some generic situation. Analysis is based on knowledge about your enemies. With *Secur/Tree* you will be able to provide a risk perspective of your local situation.

Threat Trees Grown For You

Even custom built systems use many standard components (*e.g., Oracle, Solaris, Windows 2000*). Modeling each of these systems from scratch would be a great deal of work and require specialized knowledge. *Secur/Tree* provides a library† of trees which you can include in your models. The default library trees can be easily tailored to match your local configuration. Libraries are regularly updated to keep pace with new threats or as new versions of products are released. These libraries are available to *Secur/Tree* customers as part of our library subscription program.

Tree Recycling

Secur/Tree allows you to create libraries that reflect the customized configuration of the components at your site. This allows you, and others in your organization, to apply previous work to new problems.

† For complete program details please contact your Amenaza representative.

Strong Roots for Decision-Making

Ensure that your risk management decisions are rooted in a systematic, logical process which involves all stakeholders. *Secur/Tree* makes it happen:

- **KNOWLEDGE:** Exhaustively model your IT risk environment.
- **INVOLVEMENT:** Incorporate IT and corporate management risk assessment input.
- **DECISION SUPPORT:** Use completed threat trees to determine and support the decision making process. Who will attack? What weaknesses could they exploit? Should we mitigate the risk? How can we close the holes in the system?
- **DELEGATION:** Trees are natural delegation tools; assign branches of the model (sub-trees) to relevant functional areas.
- **REPORTING:** Trees grow with new risks; trees are pruned as risks are addressed... you will always know where you stand and others will too.

Dedicated Roots

At **Amenaza Technologies** we are committed to achieving excellence in every aspect of our business. Whether it be technical support, library maintenance, customer service... we will work with you to get the most out of our products and services.