HARRIS

STAT® Analyzer

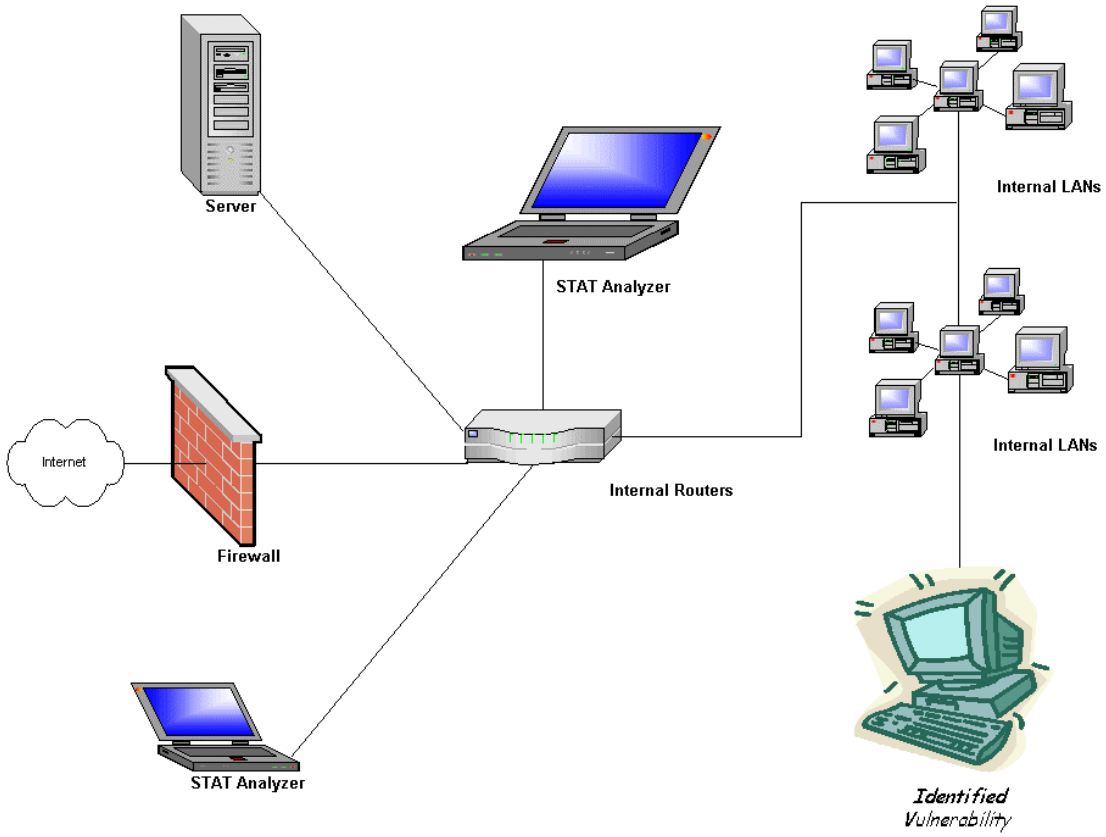
Product Guide

STAT®
SECURITY THREAT AVOIDANCE TECHNOLOGY

Introduction to STAT® Analyzer

The Importance of a Security Assessment

Today's computer networks have become increasingly complex, which in turn increases the potential number of vulnerabilities. The need for accurate, available, and protected data has become critical to businesses in light of continually growing threats of attack from malicious hackers. Enforcing security policies and maintaining a healthy computing system are critical to company operations, since security breaches can be very costly. By examining each and every element of a network for vulnerabilities according to a company's existing security policies, a picture begins to emerge of how best to protect these assets.



Vulnerabilities can appear in any part of the network, at any point of contact

The importance of performing a security assessment can be compared to that of securing a home. A smart homeowner who is concerned with protecting an investment would be wise to regularly inspect a home for potential security problems. These problems (vulnerabilities) could be logistical (configuration) in nature; for example, the existence of landscaping that could shield a potential intruder from view. Perhaps a defect (bug) exists in the system, such as an easily broken door lock. Or maybe a problem exists with a set of rules (policy), such as family members not having been instructed to lock all doors and windows when leaving the house. In an ideal world, the homeowner would have a tool available that would identify all the vulnerabilities in the home, giving the homeowner insight into how an intruder might gain unauthorized entry. While a homeowner might not consider every piece of data critical, consider this same information placed into in the hands of an experienced intruder (hacker). Suddenly, the scenario becomes quite serious.

Would a concerned homeowner lock the front door and back door but leave the windows unsecured? The worst possible security breach in a house would be an intruder gaining access, taking control of the house. The worst possible security breach in a computer network would be an intruder gaining *root access*, or domain administration rights over an entire system.

Security engineers responsible for conducting security assessments on enterprise systems face the daunting task of mapping a company's network, then running one or more vulnerability tools on each component of the network, and then making sense out of a large volume of the resulting information. A single tool that combines the results of multiple vulnerability assessment tools plus simulates an attack on a model of a company's network, much like a malicious hacker would, could bring hidden problems to light. The use of a single graphical user interface to perform this assessment would also considerably reduce the amount of time required for a security engineer to run the tools.

Harris Corporation has recognized the need for a single tool interface, and offers STAT® Analyzer, which integrates commercially available tools to produce a single, unified output. Powered by the FuzzyFusion™ engine, *reasoning chains* – or the sequence of steps an attacker might take during an attack – provide unique insight into vulnerability exploitation scenarios. The reasoning chains follow the sequence of hacking steps and report those results in terms of an attacker achieving root access. Users can employ STAT Analyzer's extensive reporting capability to draw their own conclusions as to the health of their system, and make the necessary fixes to achieve robustness.

What is STAT Analyzer?

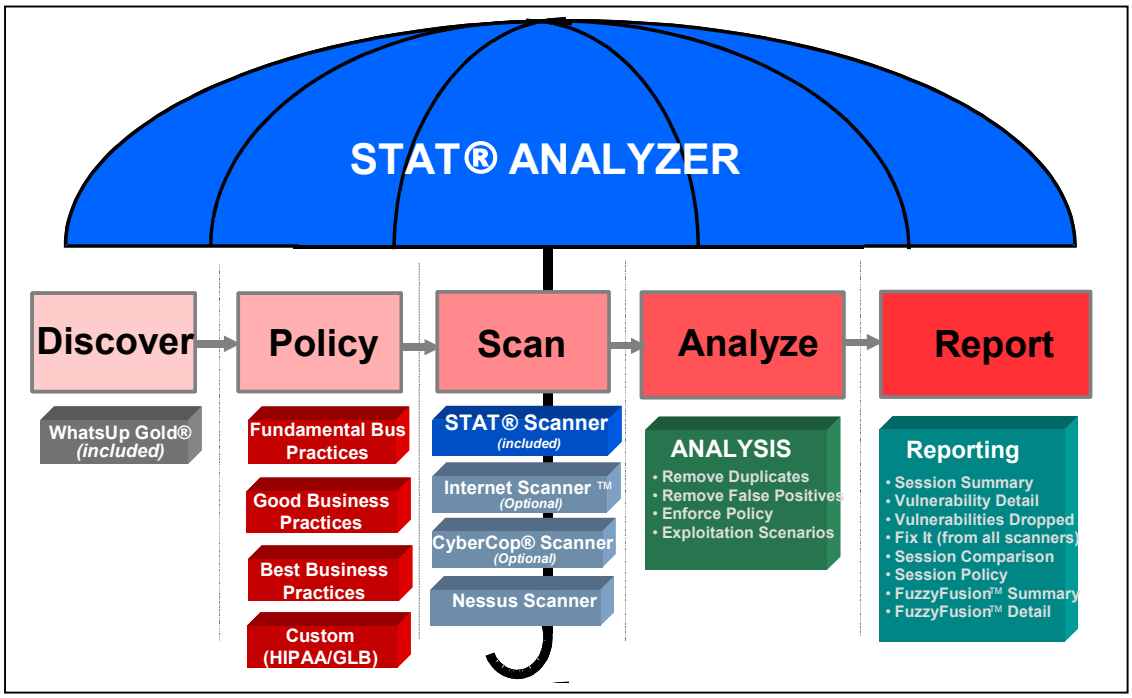
STAT Analyzer is one of the first network security tools of its kind that automates and streamlines the network security assessment process. STAT Analyzer automatically consolidates multiple tool results and provides a single, flexible reporting mechanism for reviewing those results. Rather than relying on experienced, expensive personnel to review and correlate data from multiple tools, users can take advantage of STAT Analyzer's extensive system knowledge base to consolidate outputs and immediately attack network security problems. This expert knowledge base ultimately reduces the level of security experience required, which reduces staffing costs and costly training. The STAT Analyzer Wizard walks the user through the security assessment process from start to finish.

According to *e-fense, Inc*, a third-party assessment group that has extensively evaluated the STAT Analyzer software, ***STAT Analyzer's integrated approach improves efficiency by 66%***. This increased efficiency is achieved through assessment accuracy and more consistently correlated results. FuzzyFusion, the expert reasoning engine behind STAT Analyzer, uses the user's defined security policy and detailed network information in its assessment process, correlating this data with the results of the scanning tools. This use of an enterprise's security policy in an assessment process is also the first of its kind.

Multiple, flexible, reports can be generated from an easy-to-use, graphical user interface. These reports document a company's security posture at a glance, allowing users to perform immediate fixes. Reports can also be useful to inform management of additional approaches to the enterprise's network management practices to ensure network robustness.

How does STAT Analyzer work?

The STAT Analyzer Wizard automates the security assessment process, using the five steps shown below.



The security assessment process using STAT Analyzer

The Security Assessment Process

1. Discover the Network

STAT Analyzer launches a network discovery tool, Ipswitch's WhatsUp Gold® (WUG), that defines the physical devices associated with a network, or retrieves an existing model. WhatsUp Gold is included with the STAT Analyzer software

2. Create a Security Policy

Next comes the determination of the security policy. This is carried out using the Security Policy Editor. STAT Analyzer includes a selection of four pre-defined security policies offering varying levels of security, from the most basic through more stringent to full U.S. Department of Defense C2 ('Orange Book') security standards. However, it is easy to create a custom policy simply by ticking checkboxes on a 'tree' of policy elements.

3. Scan for Vulnerabilities

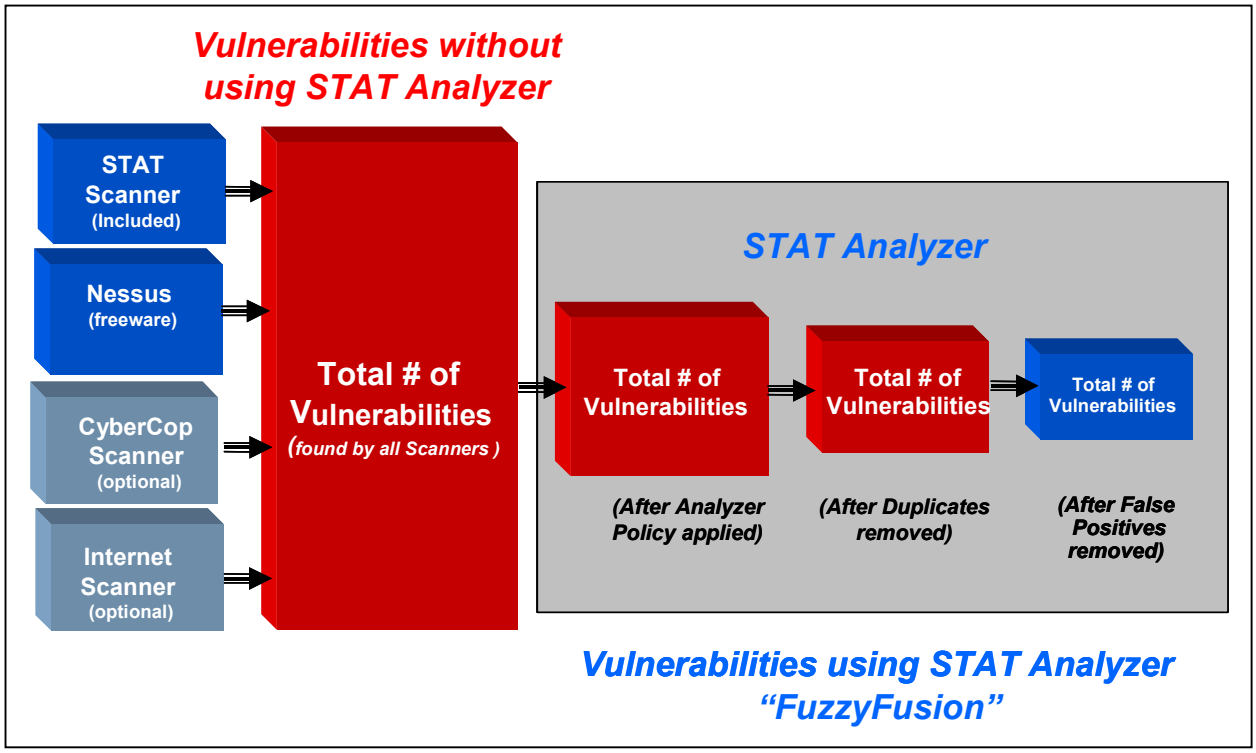
STAT Analyzer automatically runs the vulnerabilities scanners that are installed. These tools perform a security vulnerability analysis of network services and analyze the security of devices on an enterprise-wide network, checking for vulnerabilities on various types of servers, desktop systems, and firewalls. Scanner tools supported by STAT Analyzer are:

- Harris Corporation's STAT® Scanner. (Provided with STAT Analyzer. STAT Scanner detects over 2,000 vulnerabilities in the following environments: Windows NT®, Windows® 95/98/2000/Me/XP, Windows® Server 2003, Red Hat™ & Mandrake™ Linux®, Sun™ Solaris™ & HP-UX UNIX®, HP printers and Cisco® routers. STAT Scanner also provides an AutoFix capability, allowing the user to automatically fix many vulnerabilities in the system.)

- Nessus (popular freeware tool developed by Renaud Deraison)
- Internet Security System's (ISS) Internet Scanner™
- Network Associates' CyberCop Scanner®.

4. Analyze Reports Automatically

Once the scanners have completed their assessments, STAT Analyzer correlates all the results and reduces the number of vulnerabilities, as shown in the figure below.



Assessment Results using STAT Analyzer

First, the security policy (selected from STAT Analyzer's predefined templates or created by the user) is applied to the resulting vulnerabilities and all vulnerabilities not applicable to the policy are eliminated. Next, any vulnerabilities that are duplicated among the scanners are eliminated. Then, *false positives*, which are those vulnerabilities that do not apply to the user's environment, are eliminated (for example, a UNIX® vulnerability is identified but the user is operating a Windows® machine.) Once the applicable vulnerabilities have been determined, then STAT Analyzer runs FuzzyFusion to determine the severity of exposure of the accessed nodes of the network, in terms of root, user, and information access.

5. Develop Succinct, Insightful Reports

STAT Analyzer provides an extensive reporting capability. These reports are generated from an integrated database, which stores the data from *sessions*, or individual network assessments. Reports range from high-level summaries of an analysis to detailed descriptions of the vulnerabilities to actual suggestions for fixes from the vulnerability scanners. Reports are available in a summary view, which is a valuable tool for the IT manager assessing resource allocation, and in a detailed view for those network security engineers responsible for implementing fixes.

Benefits of STAT Analyzer

Feature	Benefit
Single Network Model	A network mapping tool produces a unified network model, which is then shared with all vulnerability scanners and the analysis tools.
Time Savings	The consolidated data entry and analysis of results from multiple vulnerability scanners offers considerable timesavings for security engineers performing assessments.
Increased Accuracy	The accuracy of a network security assessment is increased by the employment of multiple scanning tools. Each scanning tool has unique strengths, which ensure a wide array of results.
Customizable Security Policy	Security engineers may tailor the security policy to an enterprise's needs. STAT Analyzer applies the established policy and filters out any vulnerabilities that are not applicable, thus reducing the number of vulnerabilities a security engineer must review and address.
Reduction of False Positives	STAT Analyzer eliminates vulnerabilities that do not meet established vulnerability requirements. For example, the vulnerability may require a database server; however, if the node does not have a database server, the vulnerability is eliminated. Duplicate vulnerabilities occur among scanning tools. Instead of counting the vulnerability more than once, the duplicated vulnerability is dropped.
Batch Processing of Scanners	STAT Analyzer automatically runs the selected vulnerability scanners, allowing the user to break the scan size down into smaller scans (batches) and set a timeout which will abort the scanning of a failed batch. This feature is very useful, since vulnerability scanners often get "hung up" while scanning. STAT Analyzer allows the user to re-run any batches that fail as many times as desired to assist in performing a successful scan of the entire network.
Reasoning Chain Analysis	FuzzyFusion's reasoning chains provide exploitation scenarios that aid in identifying an enterprise's weak spots. Often, several low severity vulnerabilities, when exploited together, can lead to a high risk of root access on a system. STAT Analyzer identifies these scenarios, and arms the security engineer with this additional knowledge to aid in keeping the network secure.
Extensive Reporting Capabilities	Security engineers may use STAT Analyzer's reporting capability to highlight key information previously only created through an intensive manual effort (for example, grouping vulnerabilities by category). Reports can be printed or exported to several different file formats for distribution or information sharing. These formats include HTML 4.0, PDF (Adobe Acrobat 4.0 or higher), and XML.
Customer Care	Customer support is available through the STAT Operations Center. Visit the STAT website at http://www.*stat.harris.com*.com.

System Requirements

Hardware Requirements

- PC or compatible with Pentium® III processor or higher
- 256 MB RAM (512 recommended)
- 650 MB free disk space
- 800 x 600 monitor resolution display (1024 x 768 recommended)
- CD-ROM drive or an Internet connection

Software Requirements

- Windows NT ® 4.0 SP5 or higher; Windows® 2000; Windows ® XP
- Vulnerability scanner (STAT Scanner 5.0, Nessus, ISS Internet Scanner 6.01, or CyberCop Scanner 5.5)
- Administrative privileges on the host machine (for running STAT Analyzer, STAT Scanner)

Note: If running the Nessus scanner, the Nessus server must be installed on a Posix compatible operating system such as Linux, prior to running STAT Analyzer. The scanning user name and password are required to log onto the Nessus server. For detailed instructions on installing and configuring a Nessus server, visit the Nessus web page at http://www.nessus.org.

Summary

STAT Analyzer is Harris Corporation's network security analysis tool that integrates commercial network mapping and scanning tools to perform an assessment of an enterprise's computing system. STAT Analyzer reduces the manual labor involved through automating and correlating assessment results. According to SC Magazine "*STAT Analyzer* is the most easy to use tool for managing the vulnerability-scanning process and delivering reports. Used as a front-end to supported third-party scanners, it actually makes them easier to use and to configure. It offers an excellent solution to the problem of integrating network auto-discovery with vulnerability scanning engines. Its ability to consolidate reports from multiple scanning engines as well as providing a single interface for configuring those engines is unmatched. Used with its own *STAT Scanner*, and without further expense on third-party vulnerability scanners, it already provides a complete solution to the security management headache of keeping up with vulnerabilities and fixing them automatically."