STAT® SCANNER

PROFESSIONAL VERSION 5.08

SECURITY TARGET

DOCUMENT # 8008352

Revision C

April 7, 2003

STAT® SCANNER

PROFESSIONAL VERSION 5.08

SECURITY TARGET

DOCUMENT # 8008352

Revision C

April 7, 2003

Prepared By:		Approved By:	
Shelley White Systems Engineer	Date	Darwin Ammala Security Engineer	Date
Approved By:			
Rich Caliari Principal Investigator	Date	Sandy Terry Product Manager	Date
Reviewed By:			
Jennifer Devine Software Configuration Manager	Date	Kathy Wilder Quality Engineer	Date

HARRIS

Document 8008352
Revision C
April 7, 2003

Foreword

Harris Corporation as part of its program to promulgate security solutions for information systems issues this publication, the STAT® Scanner Security Target.

Comments on this document should be directed to Harris Corporation, Government Communications Systems Division, ATTN: STAT, P.O. Box 37, Palm Bay, Florida 32902

HARRIS

Document 8008352
Revision C
April 7, 2003

REVISION HISTORY AND RECORD

Revision	Description of Change	Authority	Date
-	Initial Release		January 21, 2003
A	PTRDOC 495 Evaluator and Certifier Observation Reports and Clarification Reports addressed.		March 5, 2003
B	PTRDOC 551		March 25, 2003
C	PTRDOC 588 – updated to reflect Evaluator and Certifier Observation Report		April 7, 2003

Table of Contents

List of Tables

List of Figures

1 INTRODUCTION

This introductory section presents *security target (ST)* identification information and an overview of the ST structure. A brief discussion of the ST development methodology is also provided.

An ST document provides the basis for the evaluation of an *information technology (IT)* product or system (e.g., target of evaluation (TOE)). An ST principally defines:

- A set of assumptions about the security aspects of the environment, a list of threats which the product is intended to counter, and any known rules with which the product must comply (in Section 3, Security Environment).
- A set of security objectives and a set of security requirements are presented in Sections 4 and 5, Security Objectives and IT Security Requirements, respectively.
- The IT security functions provided by the TOE which meet that set of requirements (in Section 6, TOE Summary Specification).

The structure and contents of this ST comply with the requirements specified in the CC, Part 1, Annex C, and Part 3, Chapter 5.

1.1 Identification

Title: STAT® Scanner Professional Version 5.08 Security Target

Evaluation Assurance Level (EAL): This TOE is CC *Part 2 extended* and *Part 3 augmented*, with a claimed Evaluation Assurance Level of EAL2 Augmented. No security functional requirement beyond those in the United States Department of Defense Intrusion Detection System Scanner Protection Profile is claimed. The following augmentations are claimed: ACM_CAP.4, ACM_SCP.1, ALC_DVS.1, ALC_FLR.3, ALC_LCD.1, AVA_MSU.1

Protection Profile Conformance: The Harris STAT® Scanner Professional Version 5.08 conforms with the IDS Scanner Protection Profile, Version 1.1, December 10, 2001.

Common Criteria Identification: Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999.

International Standard**:** ISO/IEC 15408:1999.

Keywords: intrusion detection, intrusion detection system, sensor, scanner, and analyzer

Related Protection Profiles

These Protection Profiles are for IDS components and the IDS system itself. They are included for reference only, and no conformance is claimed.

Intrusion Detection System Analyzer Protection Profile
Intrusion Detection System Sensor Protection Profile
Intrusion Detection System Protection Profile

1.2 Conventions, Terminology, and Acronyms

This section identifies the formatting conventions used to convey additional information and terminology having specific meaning. It also defines the meanings of abbreviations and acronyms used throughout the remainder of the document.

1.2.1 Conventions

This section describes the conventions used to denote CC operations on security requirements and to distinguish text with special meaning. The notation, formatting, and conventions used in this ST are largely consistent with those used in the CC. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows several operations to be performed on functional requirements; *assignment, iteration, refinement*, and *selection* are defined in paragraph 2.1.4 of Part 2 of the CC.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment is indicated by showing the value in square brackets [assignment_value(s)].
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.
- The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by <u>*underlined italicized text*</u>.
- Plain *italicized text* is used for both official document titles and text meant to be emphasized more than plain text.

1.2.2 Terms

This section describes terms that are used throughout the STAT® Scanner Security Target (ST) and reflects the terms used in the IDS PP family to maintain consistency. When possible, terms are defined as they exist in the *Common Criteria for Information Technology Security Evaluation* or the *NSA Glossary of Terms Used in Security and Intrusion Detection* provided by the NSA Information Systems Security Organization. The definitions were modified only to provide consistency with the Intrusion Detection System Scanner Protection Profile. For example, occurrences of *computer system* or *network* were replaced with IT System. The authors of the STAT® Scanner ST defined all other terms as necessary.

- **Assets** - Information or resources to be protected by the countermeasures of a TOE,

- **Attack** - An attempt to bypass security controls on an IT System. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the IT System and the effectiveness of existing countermeasures,

- **Audit** - The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend indicated changes in controls, policy, or procedures,

- **Audit Trail** - In an IT System, a chronological record of system resource usage, this includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized,

- **Authentication** - To establish the validity of a claimed user or object,

- **Authorized Administrator** - A subset of authorized users that manage an IDS component. For the purposes of the TOE, all authorized users manage an IDS component. Therefore, the set of authorized administrators is equal to the set of authorized users,

- **Authorized User** - A user that is allowed to perform IDS functions and access data. For the purposes of the TOE, all users also manage an IDS component,

- **Availability** - Assuring information and communications services will be ready for use when expected,

- **Compromise** - An intrusion into an IT System where unauthorized disclosure, modification or destruction of sensitive information may have occurred,

- **Confidentiality** - Assuring information will be kept secret, with access limited to appropriate persons,

- **Evaluation** - Assessment of a PP, a ST or a TOE, against defined criteria,

- **IDS component** - A Sensor, Scanner, or Analyzer,

- **Information Technology (IT) System** - May range from a computer system to a computer network,

- **Integrity** - Assuring information will not be accidentally or maliciously altered or destroyed,

- **Intrusion** - Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource,

- **Intrusion Detection (ID)** - Pertaining to techniques that attempt to detect intrusion into an IT System by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network,

- **Intrusion Detection System (IDS)** - A combination of Sensors, Scanners, and Analyzers that monitor an IT System for activity that may inappropriately affect the IT System's assets and react appropriately,

- **Intrusion Detection System Analyzer (Analyzer)** - The component of an IDS that accepts data from Sensors, Scanners and other IT System resources, and then applies analytical processes and information to derive conclusions about intrusions (past, present, or future),

- **Intrusion Detection System Scanner (Scanner) -** The component of an IDS that collects static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System,

- **Intrusion Detection System Sensor (Sensor)** - The component of an IDS that collects real-time events that may be indicative of vulnerabilities in or misuse of IT resources,

- **IT Product** - A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems,

- **Network** - Two or more machines interconnected for communications,

- **Protection Profile (PP)** - An implementation-independent set of security requirements for a category of TOE that meet specific consumer needs,

- **Scanner data** - Data collected by the Scanner functions,

- **Scanner functions** - The active part of the Scanner responsible for collecting configuration information that may be representative of vulnerabilities in and misuse of IT resources (i.e., Scanner data),

- **Security** - A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences,

- **Sensor data** - Data collected by the Sensor functions,

- **Sensor functions** - The active part of the Sensor responsible for collecting information that may be representative of vulnerabilities in and misuse of IT resources (i.e., Sensor data),

- **Security Policy** - The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information,

- **Security Target (ST)** - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE,

- **Target of Evaluation (TOE)** - An IT product of system and its associated administrator and user guidance documentation that is the subject of an evaluation,

- **Threat** - The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. A potential violation of security,

- **TOE Security Functions (TSF)** - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP,

- **TOE Security Policy (TSP)** - A set of rules that regulate how assets are managed, protected, and distributed within a TOE,

- **TSF data** - Data created by and for the TOE that might affect the operation of the TOE,

- **TSF Scope of Control (TSC)** - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP,

- **User** - Any entity (human user or external IT entity) outside the TOE that interacts with the TOE,

- **Vulnerability** - Hardware, firmware, or software flaw that leaves an IT System open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth that could be exploited by a threat to gain unauthorized access to information, unauthorized privileges, or disrupt critical processing.

1.2.3 Acronyms

ACL	Access Control List
CC	Common Criteria
CM	Configuration Management
EAL	Evaluation Assurance Level
IDS	Intrusion Detection System
IDSSPP	Intrusion Detection System Scanner Protection Profile
IP	Internet Protocol
IT	Information Technology
LSA	Local Security Authority
NIC	Network Interface Card
NTLM	NT LAN Manager
OS	Operating System
PP	Protection Profile
SAM	Security Account Manager
SFR	Security Functional Requirement
SOF	Strength of Function
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target

STAT	Security Threat Avoidance Technology
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

1.3 Overview

An Intrusion Detection System (IDS) monitors an IT System for activity that may inappropriately affect the IT System's assets. An IT System may range from a computer system to a computer network.

An IDS consists of Sensors, Scanners and Analyzers. Sensors and Scanners collect information regarding IT System activity and vulnerabilities, and they forward the collected information to Analyzers. Analyzers perform intrusion analysis and reporting of the collected information.

The STAT® Scanner Professional Version 5.08 product (hereafter referenced as STAT® Scanner) supports the ability to statically monitor a set of IT resources in order to identify events that may be indicative of potential vulnerabilities in or misuse of those IT resources. Through the use of Windows® operating system resources and IT administration best practices for code and data protection, the TOE protects itself, its associated data, and output report database from unauthorized access or modification and ensures accountability for authorized actions. Additionally, as a secondary data disclosure protection measure, STAT® Scanner provides cryptographic protection for vulnerability identification data and external host authentication data. This feature is transparent to the user, and is not controllable or tunable by the user. The cryptographic protection is accomplished through encryption software. Note that the cryptographic data protection services within STAT® Scanner are not within the scope of the Common Criteria evaluation to which this ST applies.

The STAT® Scanner product provides for a level of protection which is appropriate for IT environments that require detection of vulnerable software and evidence of malicious attempts to gain inappropriate access to IT resources, where the STAT® Scanner can be appropriately protected from hostile attacks. A claim of SOF-basic is made. STAT®

Scanner can be used to monitor a system or network in a hostile environment, but it is not designed to resist direct, hostile attacks. The STAT® Scanner ST does not fully address the threats posed by malicious administrative or system development personnel. This ST is also not intended to result in a product that is foolproof and able to detect intrusion attempts by hostile and well-funded attackers. The STAT® Scanner product is suitable for use in both commercial and government environments.

The STAT® Scanner Security Target was constructed to provide a target metric for consumer comparison and evaluation of STAT® Scanner against other vulnerability and intrusion scanners. This ST identifies security functions and assurances that represent the security requirements addressed by the STAT® Scanner product.

It should be noted that just because STAT® Scanner is conformant with this Security Target, STAT® Scanner should not be assumed to be interoperable with any other IDS component evaluated against another Security Target or Protection Profile in the Intrusion Detection System family of Protection Profiles. There are no requirements for interoperability within the Intrusion Detection System Family of Protection Profiles.

1.4 References

[1] Common *Criteria for Information Technology Security Evaluation*, CCIMB-99-031, Version 2.1, August 1999.
[2] NSA *Glossary of Terms Used in Security and Intrusion Detection*, Greg Stocksdale, NSA Information Systems Security Organization, April 1998.

2 DESCRIPTION

The TOE description aims to aid the understanding of the TOE security requirements and provides a context for the evaluation. It defines the scope and boundaries of the TOE, both physically and logically, and describes the environment into which the TOE will fit.

2.1 Intended Use

STAT® Scanner collects static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion on an IT System. The information collected is obtained from a variety of sources located on an IT System.

In general, STAT® Scanner collects relevant information from one or more sources and manages that information until it can be delivered to analysis functions. The STAT® Scanner does not perform analysis on the information that it collects beyond comparison against known secure settings and versions. An Analyzer such as STAT® Analyzer performs analysis functions, such as relating the vulnerability found to the larger system wide perspective. STAT® Scanner performs the following functions:

- Collect static configuration information about an IT System, where configuration information may include detected malicious code, access control configuration, service configuration, authentication configuration, accountability policy configuration, and detected known vulnerabilities.
- Protect itself and its data from tampering.
- When invoked from STAT® Analyzer forward all collected configuration information to STAT® Analyzer for data reduction and analysis.
- Forward all collected information to a remote STAT® Console for centralized collection and reporting.
- Ensure that only authorized users have the ability to configure Scanning behavior.
- Produce an audit trail (e.g., configuration changes, STAT® Scanner and data accesses).

STAT® Scanner's functionality compliments that of an IDS. Any IT System that needs to be aware of vulnerabilities and cyber attacks should deploy an IDS along with one or more STAT® Scanners.

The IT System must provide adequate protection for the STAT® Scanner so that the STAT® Scanner operates in a non-hostile environment. The following diagrams illustrate examples of how STAT® Scanner (represented by a star) may be utilized by IT Systems ranging from a computer system to a computer network.
Figure 2-1 illustrates that STAT® Scanner may monitor and exist in a computer system that is not necessarily part of a larger network – e.g., on a standalone Windows® host.
Figure 2-2 illustrates that STAT® Scanner may monitor and exist within a computer network. The arrows represent the assessment functionality of STAT® Scanner as opposed to the communication paths of the computer network.

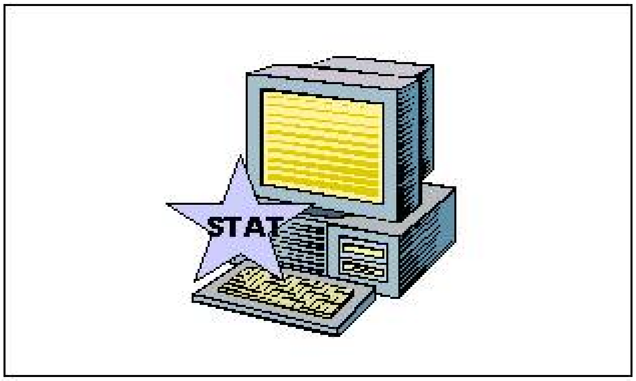

Figure 2-1 STAT® Scanner Assessing its Windows® Host

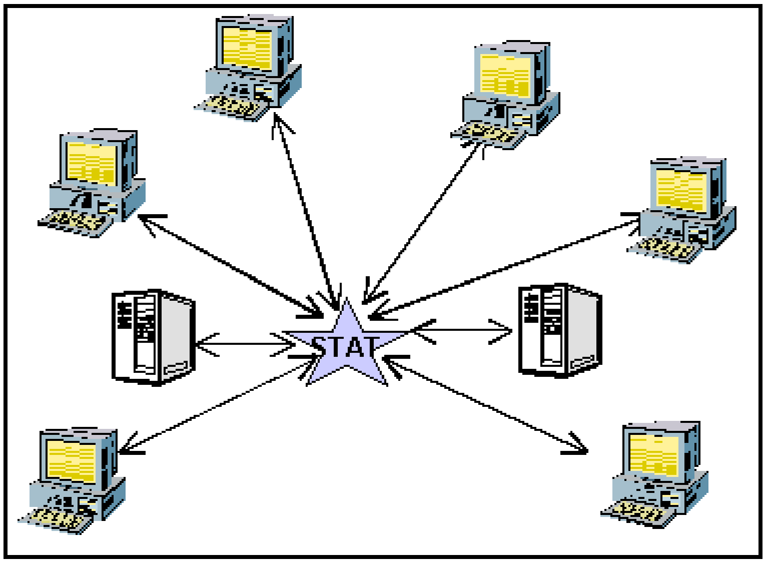

Figure 2-2 STAT® Scanner Assessing a Network

2.2 Target of Evaluation

2.2.1 Target of Evaluation

This section defines the Target of Evaluation. The evaluated configuration comprises: the STAT® Scanner software, a Windows® 2000 platform with supporting devices including a Network Interface Card (NIC), and user guidance documentation describing the correct configuration and operation of the TOE. The correct configuration is described in detail in STAT® Scanner User's and Installation Guide. Figure 2-3 shows the evaluated configuration and interactions when scanning remote machines.

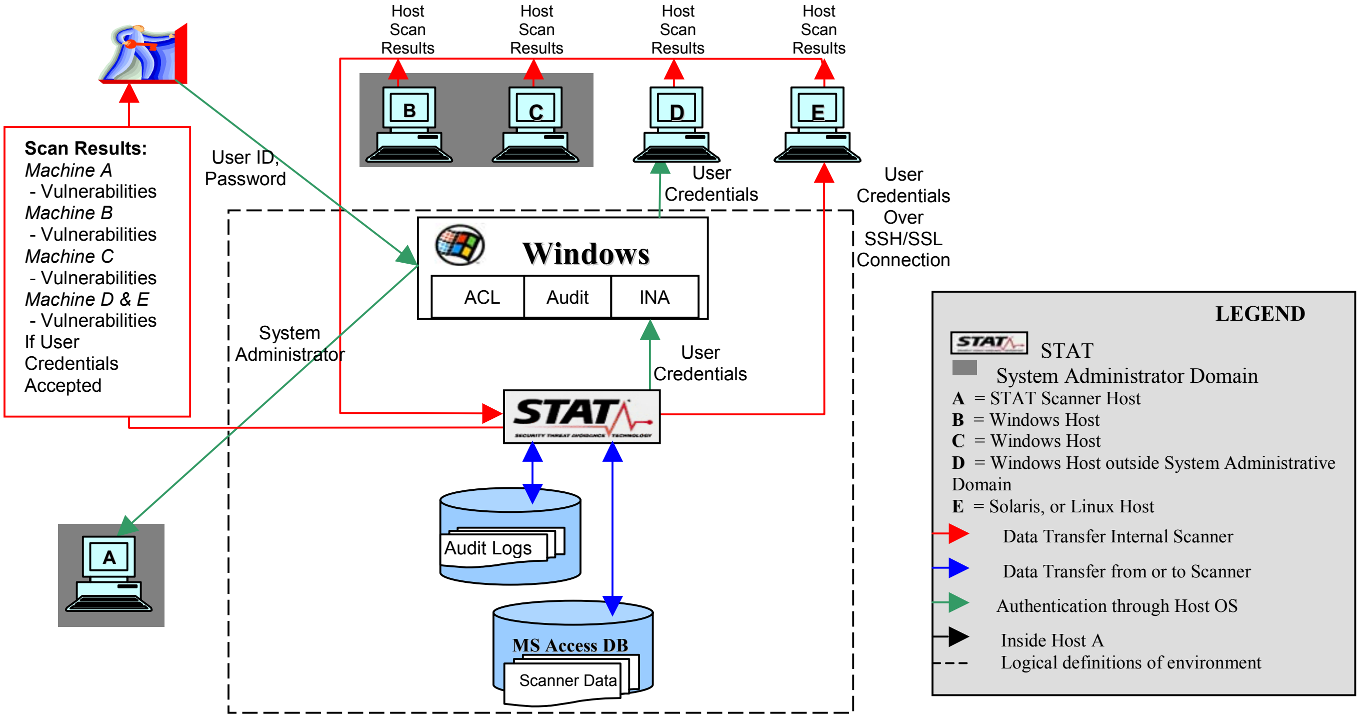

Figure 2-3 Interactions between the TOE and remote machines

2.2.2 TOE Overview

TOE security functionality is provided by the STAT® Scanner and by Windows® 2000. TOE functionality includes:

- Collection of static configuration information about an IT System, where configuration information includes detected malicious code, access control configuration, service configuration, authentication configuration, accountability policy configuration, and detected known vulnerabilities,
- Protection of itself and its data from attempts of tampering,
- When invoked from STAT® Analyzer, forwarding of all collected configuration information to STAT® Analyzer for data reduction and analysis,
- Is configured by an authorized user,
- Production of an audit trail (e.g., configuration changes, STAT® Scanner and data accesses).

Figure 2-4 TOE Boundary shows the TOE primary components. These are:

- The LSA, which is the local security authority regulating audit policy, and system auditing, along with authentication token management,

- The SAM, which is the security account manager that provides authentication validation used by LSA, and maintains system authentication related data,
- User Credentials, which are supplied by the user for remote target access,
- STAT® Scanner Data, which is created as a result of scanning,
- Audit Logs,
- Vulnerabilities Signatures.

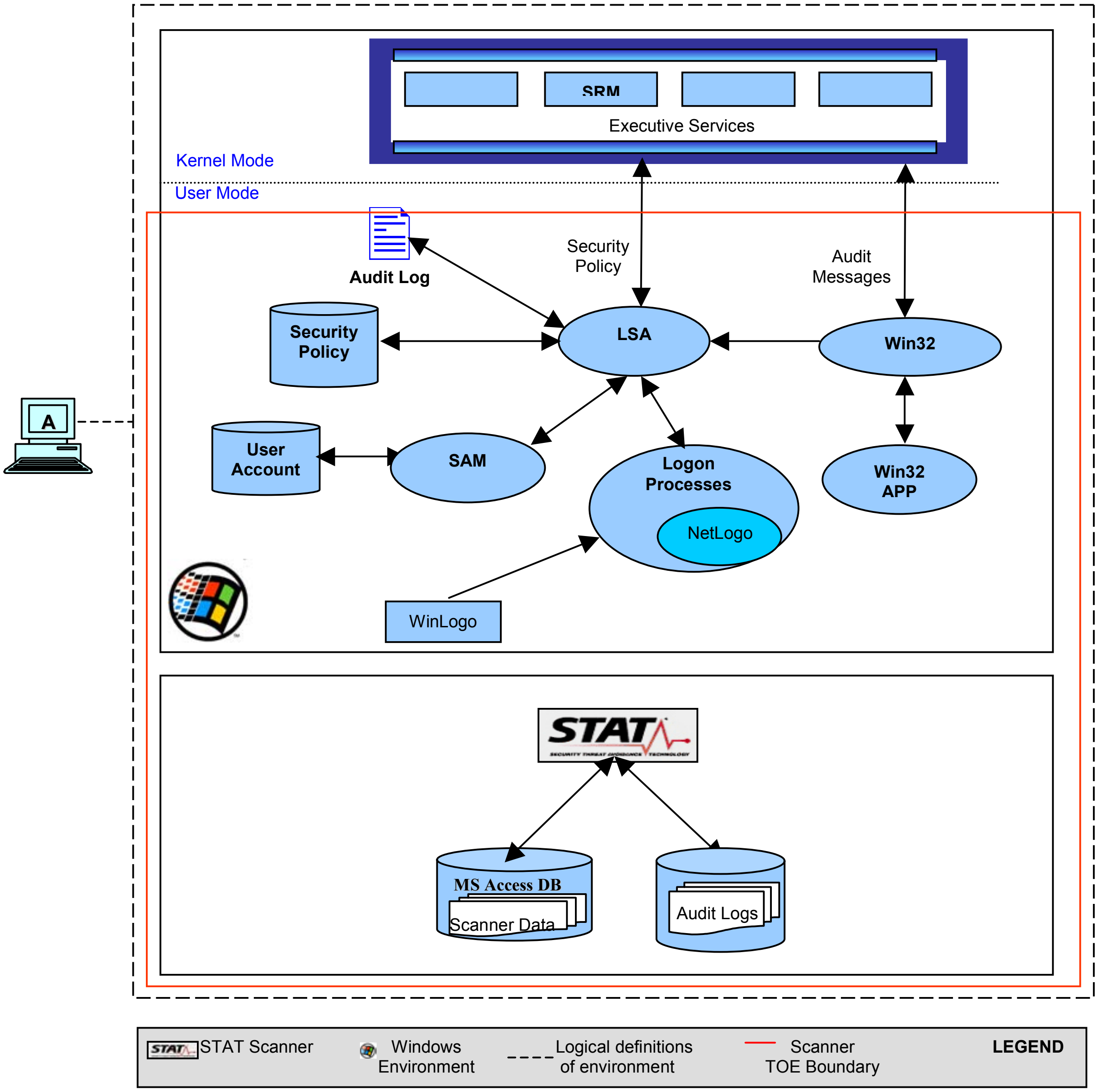

Figure 2-4 TOE Boundary

2.2.3 Identification and Authentication

STAT® Scanner provides identification and authentication of STAT® Scanner users through the Windows® operating system identification and authentication mechanisms (Winlogon), which are normally userid/password based.

2.2.4 Inter-TSF availability, confidentiality, and integrity

Inter-TSF availability, confidentiality, and integrity is provided when STAT® Scanner is executed in a networked environment, when the results of a scanning session are transmitted to a remote STAT® Console, or to a copy of STAT® Analyzer running co-located on the same host as is STAT® Scanner. Data transmitted over a network to a remote STAT® Console is protected by SSL services, to ensure confidentiality. Integrity is provided at the transport layer by TCP and at the application layer by a checksum algorithm. Data and service availability from STAT® Scanner to a co-located STAT® Analyzer is protected by the Windows® host identification/authentication service – WinLogon to ensure authenticated users only, and by the NTFS ACLs to enforce discretionary access control decisions. Data integrity between STAT® Scanner and STAT® Analyzer is provided by the Windows NTFS file system, and Microsoft Access database. Confidentiality is provided by co-location of the STAT® Scanner and STAT® Analyzer, through mutually accessible NTFS file system resources and by ACL settings of the file system resources.

2.2.5 Scanner data collection

Scanner compares the configuration of systems against a database of vulnerability assessment information. The results of this comparison are summarized in a report of potential vulnerabilities and/or possible previous intrusions. The database of vulnerability assessment information is based on the knowledge of the STAT® team of security engineers who have researched security advisories, knowledge base papers, and professional security group articles to provide a single source of vulnerability information.

3 SECURITY ENVIRONMENT

3.1 Introduction

The statement of TOE security environment describes the security aspects of the intended usage environment for the TOE and the manner in which it should be employed.

The statement of TOE security environment identifies the assumptions made on the operational environment (including physical and procedural measures) and the intended method of use for the product, defines the threats that the product is designed to counter, and defines the organizational security policies with which the product is designed to comply.

3.2 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

3.2.1 Intended Usage Assumptions

A.ACCESS The TOE has access to all the IT System data it needs to perform its functions.

A.DYNMIC The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

A.ITSYSCOR The TOE depends on the correct functioning of the IT System including:

a. Domain Controller
b. Unix system security access components
c. Windows® system security access components, and
d. Network infrastructure and mapping.

(This assumption did not originate from Intrusion Detection System Scanner Protection Profile)

A.ASCOPE The TOE is appropriately scalable to the IT System the TOE monitors.

3.2.2 Physical Assumptions

A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

3.2.3 Personnel Assumptions

A.MANAGE There will be one or more individuals assigned to manage the TOE and the security of the information it contains. The assigned personnel possess experience in supporting and maintaining all aspects of the TOE and the encompassing IT environment.

A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.NOTRST The TOE can only be accessed by authorized users.

3.3 Threats

The following are threats identified for the TOE. The TOE itself has threats and the TOE is responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for these threats is unsophisticated.

3.3.1 TOE Threats

T.COMINT An unauthorized user may attempt to compromise the integrity of the data collected by the TOE by bypassing a security mechanism.

T.COMDIS An unauthorized user may attempt to disclose the data collected by the TOE by bypassing a security mechanism.

T.LOSSOF An unauthorized user may attempt to remove or destroy data collected by the TOE.

T.NOHALT An unauthorized user may attempt to compromise the continuity of the STAT® Scanner’s collection functionality by halting execution of the TOE.

T.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

T.IMPCON An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

T.INFLUX An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

T.FACCNT Unauthorized attempts to access TOE data or security functions may go undetected.

3.3.2 IT System Threats

The following identifies threats to the IT System that may be indicative of vulnerabilities in or misuse of IT resources.

T.SCNCFG Improper security configuration settings may exist in the IT System the TOE monitors.

T.SCNMLC Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.

T.SCNVUL Vulnerabilities may exist in the IT System the TOE monitors.

3.4 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs.

P.DETECT Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System must be collected.

P.MANAGE The TOE shall be managed only by authorized users.

P.ACCESS All data collected by the TOE shall only be used for authorized purposes.

P.ACCACT Users of the TOE shall be accountable for their actions within the IDS.

P.INTGTY Data collected by the TOE shall be protected from modification.

P. PROTCT The TOE shall be protected from unauthorized accesses and disruptions of collection activities.

4 SECURITY OBJECTIVES

4.1 Introduction

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

4.2 Information Technology (IT) Security Objectives

The information technology security objectives for the TOE are as defined in the IDS Scanner Protection Profile (IDSSPP). No additional security functional requirements have been added beyond those in the PP. The following are the TOE security objectives:

O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.

O.IDACTS The STAT® Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.

O.EADMIN The TOE must include a set of functions that allow effective management of its functions and data.

O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.

O.IDAUTH The TOE must be able to identify and authenticate users before allowing access to TOE functions and data.

O.OFLOWS The TOE must appropriately handle potential audit and STAT® Scanner data storage overflows.

O.AUDITS The TOE must record audit records for data accesses and use of the STAT® Scanner functions.

O.INTEGR The TOE must ensure the integrity of all audit and STAT® Scanner data.

O.EXPORT When the TOE makes its STAT® Scanner data available to other IDS components, the TOE will ensure the confidentiality of the STAT® Scanner data.

4.3 Security Objectives for the Environment

The TOE operating environment must satisfy the following objectives.
These objectives do not levy any IT requirements. These objectives are satisfied by procedural or administrative measures.

O.INSTAL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.

O. PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

O.CREDEN Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner that is consistent with IT security.

O.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the STAT® Scanner.

O.INTROP The TOE is interoperable with the IT System it monitors and other IDS components within its IDS.

5 IT SECURITY REQUIREMENTS

5.1 TOE Security Requirements

5.1.1 TOE Security Functional Requirements

The functional security requirements for the ST consist of the following components, summarized in Table 5-1 TOE Security Functional Components. The security functional requirements for the TOE are as defined in the IDS Scanner Protection Profile (IDSSPP) with selections and assignments performed to SFRs that are completed by the ST author. No additional security functional requirements have been added beyond those in the PP. The following table lists the classes, families, components and elements defined in the IDSSPP.

Table 5-1 TOE Security Functional Components

Class	Family	Component	Element	Element Description
FAU	FAU_GEN	FAU_GEN.1	FAU_GEN.1.1	Audit data generation
			FAU_GEN.1.2	Audit content
	FAU_SAR	FAU_SAR.1	FAU_SAR.1.1	Audit review
			FAU_SAR.1.2	Human readable output
		FAU_SAR.2	FAU_SAR.2.1	Restricted audit review
		FAU_SAR.3	FAU_SAR.3.1	Selectable audit review
	FAU_SEL	FAU_SEL.1	FAU_SEL.1.1	Selective audit
	FAU_STG	FAU_STG.2	FAU_STG.2.1	Unauthorized deletion detection
			FAU_STG.2.2	Detection of audit modification
			FAU_STG.2.3	Protection against loss
		FAU_STG.4	FAU_STG.4.1	Prevention of audit data loss
FIA	FIA_AFL	FIA_AFL.1	FIA_AFL.1.1	Authentication failure handling
			FIA_AFL1.2	Actions on authentication failure
FIA	FIA_UAU	FIA_UAU.1	FIA_UAU.1.1	Timing of authentication
			FIA_UAU.1.2	Permitting TSF- mediated actions
	FIA_ATD	FIA_ATD.1	FIA_ATD.1.1	User attribute definition
	FIA_UID	FIA_UID.1	FIA_UID.1.1	Timing of identification
			FIA_UID.1.2	TSF-mediated actions and identification
FMT	FMT_MOF	FMT_MOF.1	FMT_MOF.1.1	Management of security functions behavior
	FMT_MTD	FMT_MTD.1	FMT_MTD.1.1	Management of TSF data
	FMT_SMR	FMT_SMR.1	FMT_SMR.1.1	Security roles
			FMT_SMR.1.2	Association of Users with Roles
FPT	FPT_ITA	FPT_ITA.1	FPT_ITA.1.1	Inter-TSF availability within a defined availability metric
	FPT_ITC	FPT_ITC.1	FPT_ITC.1.1	Inter-TSF confidentiality during transmission
	FPT_ITI	FPT_ITI.1	FPT_ITI.1.1	Inter-TSF detection of modification
			FPT_ITI.1.2	Verification of integrity
	FPT_RVM	FPT_RVM.1	FPT_RVM.1.1	Non-bypassability of the TSP
	FPT_SEP	FPT_SEP.1	FPT_SEP.1.1	TSF domain separation
			FPT_SEP.1.2	Separation of domains between subjects
	FPT_STM	FPT_STM.1	FPT_STM.1.1	Reliable timestamps
IDS	IDS_SCN	IDS_SCN.1	IDS_SCN.1.1	Scanner Data Collection

Class	Family	Component	Element	Element Description
			IDS_SCN.1.2	Minimum Collected Events
	IDS_RDR	IDS_RDR.1	IDS_RDR.1.1	Restricted Data Review
			IDS_RDR.1.2	Human Readable Output
			IDS_RDR.1.3	Authorized Users
	IDS_STG	IDS_STG.1	IDS_STG.1.1	Guarantee of Scanner Data Availability
			IDS_STG.1.2	Unauthorized Deletion
			IDS_STG.1.3	Unauthorized Modification
		IDS_STG.2	IDS_STG.2.1	Prevention of Scanner data loss

5.1.1.1 Security Audit (FAU)

5.1.1.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the *basic* level of audit; and

c) [Access to the Scanner and access to the TOE and Scanner data]

Table 5-2 Auditable Events

Component	Event	Details
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to Scanner[1]	
FAU_GEN.1	Access to the TOE Scanner data	**Object IDS, Requested access**
FAU_SAR.1	Reading of information from the audit records	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	
FAU_STG.4	Actions taken due to the audit storage failure	
FIA_UAU.1	All use of the authentication mechanism	**User identity, location**
FIA_UID.1	All use of the user identification mechanism, including the user identity provided	**User identity, location**
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMR.1	Modifications to the group of users that are part of a role[3].	**User identity**
FPT_ITA.1	The absence of Inter-TSF data when required by the TOE	

[1] [3]. The only role within STAT® Scanner requires administrative privilege, and STAT® Scanner is a single-user application.

Component	Event	Details
FPT_ITI.1	The action taken upon detection of modification of transmitted Inter-TSF data	
FPT_STM.1	Changes to the time	

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [the additional information specified in the Details column of Table 5-2 Auditable Events]. FAU_GEN.1.2

5.1.1.1.2 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [authorized users] with the capability to read [date and time of the event, type of event, subject identity, and the outcome of the event (success or failure)] from the audit records. FAU_SAR.1.1

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information. FAU_SAR.1.2

5.1.1.1.3 FAU_SAR.2 Restricted audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access. FAU_SAR.2.1

5.1.1.1.4 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform *sorting* of audit data, based on [date and time, subject identity, type of event, and success or failure of related event]. FAU_SAR.3.1

5.1.1.1.5 FAU_SEL.1 Selective audit

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) *Event type*;

b) [Subject identity]. FAU_SEL.1.1

5.1.1.1.6 FAU_STG.2 Guarantees of audit data availability

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorized deletion. FAU_STG.2.1

FAU_STG.2.2 The TSF shall be able to *detect* modifications to the audit records. FAU_STG.2.2

FAU_STG.2.3 The TSF shall ensure that [the user specified number of kilobytes of] audit records will be maintained when the following conditions occur: *audit storage exhaustion, failure*. FAU_STG.2.3

5.1.1.1.7 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall *prevent auditable events, except those taken by the authorized user with special rights* and [send an alarm] if the audit trail is full. FAU_STG.4.1

5.1.1.2 Identification and Authentication (FIA)

5.1.1.2.1 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow [no action] on behalf of the user to be performed before the user is authenticated. FIA_UAU.1.1

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. FIA_UAU.1.2

5.1.1.2.2 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [a settable, non-zero number] of unsuccessful authentication attempts occur related to [external IT products attempting to authenticate]. FIA_AFL.1.1

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent the offending external IT product from successfully authenticating until an authorized administrator takes some action to make authentication possible for the external IT product in question]. FIA_AFL.1.2

5.1.1.2.3 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

[

a) User identity;
b) Authentication data;
c) Authorizations; and,
d) No additional. FIA_ATD.1.1

]

5.1.1.2.4 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [no action] on behalf of the user to be performed before the user is identified. FIA_UID.1.1

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. FIA_UID.1.2

5.1.1.3 Security Management (FMT)

5.1.1.3.1 FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to *modify the behavior of* the functions of [Sensor data collection and review] to [authorized Scanner administrators]. FMT_MOF.1.1

5.1.1.3.2 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to *query* [and add Scanner and audit data, and shall restrict the ability to query and modify all other TOE data] to [authorized users]. FMT_MTD.1.1

5.1.1.3.3 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the following roles: [authorized Scanner administrators]. FMT_SMR.1.1

FMT_SMR.1.2 The TSF shall be able to associate users with roles. FMT_SMR.1.2

5.1.1.4 Protection of the TOE Security Functions (FPT)

5.1.1.4.1 FPT_ITA.1 Inter-TSF availability within a defined availability metric

FPT_ITA.1.1 The TSF shall ensure the availability of [audit and Scanner data] provided to a remote trusted IT product within [immediately upon completion of a scanning session.] Given the following conditions

[

- Reporting and audit data files are in use by Scanner during an active scanning session.
- Availability to another trusted IT product is predicated upon the correct file locking functionality.
- Audit and scanner reporting data is in conventional file format

]. FPT_ITA.1.1

.

5.1.1.4.2 FPT_ITC.1 Inter-TSF confidentiality during transmission

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission. FPT_ITC.1.1

5.1.1.4.3 FPT_ITI.1 Inter-TSF detection of modification

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [Modification detection of in-transit data shall be detected within one minute of receipt by the remote trusted IT product.]. FPT_ITI.1.1

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [a graphical or textual alert dialog message and the recording of an entry in the audit log] if modifications are detected. FPT_ITI.1.1

5.1.1.4.4 FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. FPT_RVM.1.1

5.1.1.4.5 FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects. FPT_SEP.1.1

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC. FPT_SEP.1.2

5.1.1.4.6 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use. FPT_STM.1.1

5.1.1.5 IDS Component Requirements (IDS)

5.1.1.5.1 IDS_SCN.1 Scanner Data Collection (EXP)

IDS_SCN.1.1 The Scanner shall be able to collect the following static configuration information from the targeted IT System resource(s):

a) detected *malicious code, access control configuration, service configuration, authentication configuration, accountability, policy configuration, detected known vulnerabilities*; and

b) [presence of known malicious port open]. IDS_SCN.1.1

IDS_SCN.1.2 At a minimum, the Scanner shall collect and record the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) [The additional information specified in the *Details* column of Table 5-3 Scanner Auditable Events.] (EXP) IDS_SCN.1.2

Table 5-3 Scanner Auditable Events

Component	Event	Details
IDS_SCN.1	Start-up and shutdown of audit functions	None
IDS_SCN.1	Detected malicious code	Location, identification of code
IDS_SCN.1	Access control configuration	Location, access settings
IDS_SCN.1	Service configuration	Service identification (name or port), interface, protocols
IDS_SCN.1	Authentication configuration	Account names for cracked passwords, account policy parameters
IDS_SCN.1	Accountability policy configuration	Accountability policy configuration parameters
IDS_SCN.1	Detected known vulnerabilities	Identification of the known vulnerability
IDS_SCN.1	*Presence of known malicious port open*	Port scan to survey a public list of known malicious TCP/IP ports.

5.1.1.5.2 IDS_RDR.1 Restricted Data Review (EXP)

IDS_RDR.1.1 The Scanner shall provide [authorized users] with the capability to read [Reports, Selected machine lists, Contents of Configuration files, Remote target authentication data] from the Scanner data. (EXP) IDS_RDR.1.1

IDS_RDR.1.2 The Scanner shall provide the Scanner data in a manner suitable for the user to interpret the information. (EXP) IDS_RDR.1.2

IDS_RDR.1.3 The Scanner shall prohibit all users read access to the Scanner data, except those users that have been granted explicit read-access. IDS_RDR.1.3

5.1.1.5.3 IDS_STG.1 Guarantee of Scanner Data Availability (EXP)

IDS_STG.1.1 The Scanner shall protect the stored Scanner data from unauthorized deletion. IDS_STG.1.1

IDS_ STG.1.2 The Scanner shall protect the stored Scanner data from modification. (EXP) IDS_STG.1.2

IDS_ STG.1.3 The Scanner shall ensure that [all previously saved] Scanner data will be maintained when the following conditions occur: *Scanner data storage exhaustion and failure*. IDS_STG.1.3

5.1.1.5.4 IDS_STG.2 Prevention of Scanner data loss (EXP)

IDS_STG.2.1 The Scanner shall *prevent Scanner data, except those taken by an authorized user with special rights* and send an alarm if the storage capacity has been reached.[2] (EXP) IDS_STG.2.1

5.1.2 TOE Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented. Table 5-4 Assurances Classes and Components summarizes the components. For completeness, both EAL2 and augmentation requirements are included in Table 5-4. Table 5-5 Augmented TOE Assurance Requirements summarizes augmented assurance requirements.

Table 5-4 Assurances Classes and Components

Assurance Class	Assurance Components
Class ACM: Configuration management	ACM_CAP.4 Generation support and acceptance procedures ACM_SCP.1 TOE CM Coverage
Class ADO: Delivery and operation	ADO_DEL.1 Delivery procedures ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.1 Informal functional specification ADV_HLD.1 Descriptive high-level design ADV_RCR.1 Informal correspondence demonstration
Class AGD: Guidance documents	AGD_ADM.1 Administrator guidance AGD_USR.1 User guidance
Class ALC: Life cycle support	ALC_DVS.1 Identification of security measures ALC_LCD.1 Developer Defined Life Cycle Model ALC_FLR.3 Systematic Flaw Remediation
Class ATE: Tests	ATE_COV.1 Evidence of coverage ATE_FUN.1 Functional testing ATE_IND.2 Independent testing - sample
Class AVA: Vulnerability assessment	AVA_SOF.1 Strength of TOE security function evaluation AVA_VLA.1 Developer vulnerability analysis AVA_MSU.1 Examination of Guidance

Table 5-5 Augmented TOE Assurance Requirements

Assurance Component	Component ID	Component Name
Class ACM: Configuration management	ACM_CAP.4	Configuration Items
	ACM_SCP.1	TOE CM Coverage
Class ALC: Life cycle support	ALC_DVS.1	Identification of Security Measures
	ALC_LCD.1	Developer defined Life Cycle Model
	ALC_FLR.3	Systematic Flaw Remediation
Class AVA: Vulnerability assessment	AVA_MSU.1	Examination of Guidance

5.1.2.1 Configuration Management (ACM)

5.1.2.1.1 ACM_CAP.4 Generation support and acceptance procedures

Developer action elements:

ACM_CAP.4.1D The developer shall provide a reference for the TOE.

ACM_CAP.4.2D The developer shall use a CM system.

ACM_CAP.4.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.4.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.4.2C The TOE shall be labeled with its reference.

ACM_CAP.4.3C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

ACM_CAP.4.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.4.6C The CM system shall uniquely identify all configuration items.

ACM_CAP.4.7C The CM plan shall describe how the CM system is used.

ACM_CAP.4.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.4.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.4.10C The CM system shall provide measures such that only authorized changes are made to the configuration items.

ACM_CAP.4.11C The CM system shall support the generation of the TOE.

ACM_CAP.4.12C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

Evaluator action elements:

ACM_CAP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.2.1.2 ACM_SCP.1 TOE CM coverage

Developer action elements:

ACM_SCP.1.1D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_SCP.1.1C The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, and CM documentation.

ACM_SCP.1.2C The CM documentation shall describe how configuration items are tracked by the CM system.

Evaluator action elements:

ACM_SCP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

.

5.1.2.2 Delivery and Operation (ADO)

5.1.2.2.1 ADO_DEL.1 Delivery procedures

Developer action elements:

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.2.2.2 ADO_IGS.1 Installation, generation, and start-up procedures

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.1.2.3 Development (ADV)

5.1.2.3.1 ADV_FSP.1 Informal functional specification

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.1.2.3.2 ADV_HLD.1 Descriptive high-level design

Developer action elements:

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.1.1C The presentation of the high-level design shall be informal.

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action elements:

ADV_HLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.1.2.3.3 ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.2.4 Guidance Documents (AGD)

5.1.2.4.1 AGD_ADM.1 Administrator guidance

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.2.4.2 AGD_USR.1 User guidance

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.2.5 Life Cycle Support (ALC)

5.1.2.5.1 ALC_DVS.1 Identification of security measures

Developer action elements:

ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation of evidence elements:

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Evaluator action elements:

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

5.1.2.5.2 ALC_FLR.3 Systematic flaw remediation

Developer action elements:

ALC_FLR.3.1D The developer shall document the flaw remediation procedures.

ALC_FLR.3.2D The developer shall establish a procedure for accepting and acting upon user reports of security flaws and requests for corrections to those flaws.

ALC_FLR.3.3D The developer shall designate one or more specific points of contact for user reports and inquiries about security issues involving the TOE.

Content and presentation of evidence elements:

ALC_FLR.3.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.3.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.3.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.3.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.3.5C The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.

ALC_FLR.3.6C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.3.7C The flaw remediation procedures shall include a procedure requiring timely responses for the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.

Evaluator action elements:

ALC_FLR.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.2.5.3 ALC_LCD.1 Developer defined life-cycle model

Developer action elements:

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

Content and presentation of evidence elements:

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

Evaluator action elements:

ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.2.6 Tests (ATE)

5.1.2.6.1 ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation of evidence elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Evaluator action elements:

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.2.6.2 ATE_FUN.1 Functional testing

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.2.6.3 ATE_IND.2 Independent testing - sample

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.1.2.7 Vulnerability Assessment (AVA)

5.1.2.7.1 AVA_SOF.1 Strength of TOE security Function evaluation

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level of SOF-basic.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric of SOF-basic.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

5.1.2.7.2 AVA_VLA.1 Developer vulnerability analysis

Developer action elements:

AVA_VLA.1.1D The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2D The developer shall document the disposition of obvious vulnerabilities.

Content and presentation of evidence elements:

AVA_VLA.1.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

5.1.2.7.3 AVA_MSU.1 Examination of Guidance

Developer action elements:

AVA_MSU.1.1D The developer shall provide guidance documentation.

Content and presentation of evidence elements:

AVA_MSU.1.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.1.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.1.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.1.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

Evaluator action elements:

AVA_MSU.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_MSU.1.2E The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.1.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

5.2 Security Requirements for the IT Environment

There are no security requirements placed on the IT environment.

6 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

6.1 TOE Security Functions

The TOE Security Functions are described in Table 6-1.

Table 6-1 TOE Security Functions

F.AUTH	The TOE does not allow any action to be performed on behalf of the user before the user is successfully authenticated. Each user must be successfully authenticated before any TSF-mediated action is allowed on behalf of the administrator. Authorized Scanner administrators must be authenticated before obtaining access to STAT® Scanner. This security function has a basic strength of function claim.
F.AUTHFAIL	The TOE is able to detect when a defined number of unsuccessful authentication attempts occur related to external IT products attempting to authenticate. After this defined number of unsuccessful authentication attempts, the TOE prevents the external IT product from authenticating, until the authorized Scanner administrator restores the account to an active status.
F.AUDEVT	The TOE generates an audit record for the following events: 1. Start-up and shutdown of audit functions 2. Access to STAT® Scanner 3. Access to TOE STAT® Scanner data 4. Reading of information from the audit records 5. Unsuccessful attempts to read information from the audit records 6. All modifications to the audit configuration that occur while the audit collection functions are operating 7. All actions taken during audit storage failure 8. All use of the authentication mechanism 9. All use of the user identification mechanism 10. All modifications in the behavior of the functions of the TSF 11. All modifications to the values of the TSF data 12. Modifications to the group of users that are part of a role 13. The absence of TSF data when required by the TOE 14. The action taken upon detection of modification of transmitted TSF data 15. Changes to the system time

	The events audited by the TOE are configurable based on event type and subject identity.
F.AUDINF	The TOE records the following information in each audit record: 1. date and time of the event 2. type of event 3. subject – identity 4. outcome (success/failure) of the event
F.DATAREV	The TOE provides only authorized Scanner administrators with explicit read access the capability to read the following STAT® Scanner data: reports, selected machine lists, contents of configuration files, and remote target authentication data. The TOE also provides only STAT® Scanner authorized Scanner administrators with explicit read access the ability to read the following from the audit records: date and time of event, type of event, subject identity, and the outcome of the event. This information is presented in a manner suitable for human interpretation. The audit data can be sorted based on date and time, subject identity, type of event, and success or failure of the related event. STAT® Scanner is intended to operate in a networked environment with Administrative level access and privileges. STAT® Scanner data is protected using ACL entries on STAT® Scanner resources. This mechanism will not withstand a well-funded or highly experienced and motivated attacker.
F.DATAPRO	The TOE protects the audit data and STAT® Scanner data such that it is able to detect modifications to the audit records and prevent unauthorized deletion. Upon audit storage exhaustion or failure, the TOE shall maintain a user specified number of days of audit data and the most current user specified amount of STAT® Scanner data. An alarm is sent if storage capacity is reached.
F.ROLE	The TOE shall maintain the role of authorized Scanner administrator, and be able to associate users with this role.
F.USER	The TOE maintains the following security attributes for each user: user identity, authentication data, and authorizations. These security attributes are protected by the functions within the Windows® OS. Cryptographic services are not advertised as a STAT® Scanner feature. This mechanism will not withstand a well-funded or highly experienced and motivated attacker.

F.TSFDATA	The TOE shall only allow an authorized Scanner administrator to modify the behavior of the functions of data collection and review, add STAT® Scanner and audit data, and query and modify all other TOE data. STAT® Scanner data is protected by the setting of ACL entries on STAT® Scanner resources. This mechanism will not withstand a well-funded or highly experienced and motivated attacker.
F.AVAIL	The TOE ensures the availability of audit and STAT® Scanner data provided to a remote trusted IT product immediately following the completion of a scan as long as the following conditions hold: • Reporting and audit data files are in use by STAT® Scanner during an active scanning session. • Availability to another trusted IT product is predicated upon the correct file locking functionality. • Audit and scanner reporting data is in conventional file format
F.TRANS	The TOE protects the TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission. The TOE is able to detect modification of the TSF data during transmission between the TSF and a remote trusted IT product within one minute of receipt by the remote trusted IT product. The TOE is able to verify the integrity of this transmitted data and is able to generate a graphical or textual alert dialog message and record the event in the audit log if modifications are detected.
F.NOBPASS	The TOE ensures that the TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. The Windows® 2000 OS provides reference mediation through handle enforcement. Once an access policy decision is made by the TSF, the policy is enforced via the handle enforcement checks applied every time a handle is used. Access to objects is thus assured to be consistent with the security policy.
F.DOMN	The TOE maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects, and enforces a separation between the security domains of subjects in the TSC. The Windows® 2000 OS provides a security domain to protect the TSF through hardware, the processor kernel mode, controlled state-transitions, process isolation, and memory protection. Processes are managed by the TSF kernel-mode software and have private address spaces and process context.

F.TIME	The TOE provides reliable time stamps for its own use. The Windows® 2000 OS provides functions that allow the query and setting of the hardware platform's real-time clock. The ability to change the clock is restricted to authorized administrators.
F.SCANDATA	The TOE records the date and time, type, subject identity, and the outcome of the events, detected malicious code, access control configuration, service configuration, authentication configuration, accountability policy configuration, detected known vulnerabilities, and presence of known malicious ports open.

6.2 TOE Assurance Measures

The TOE assurance measures are described in Table 6-2.

Table 6-2 TOE Assurance Measures

M.ID	The TOE incorporates a unique version identifier that can be displayed to the user.
M.CMLIST	The CM documentation includes a configuration list, which describes the uniquely identified configuration items that comprise the TOE. The CM documentation provides evidence that all of the configuration items are effectively maintained under the CM system and describes the method used to uniquely identify the configuration items. The CM system provides measures so that only authorized changes are made to the configuration items. The acceptance plan describes the procedures in place to accept modified or newly created configuration items as part of the TOE.
M.SYSTEM	The TOE shall be developed and maintained using a system to ensure only authorized changes are implemented in the evaluated version of the TOE. A list of all TOE documentation shall be maintained.
M.GETTOE	The developer uses a process whereby the developer can ensure an unmodified and complete TOE has been received by the customer. This process is documented.
M.SETUP	The developer provides documentation for procedures used for secure installation, generation, and start-up of the TOE.

M.SPEC	An internally consistent, high level design, functional specification, and product description are provided. The high-level design documentation identifies the underlying hardware, firmware, and software required by the TSF. The high-level design also identifies all interfaces to the subsystems of the TSF and which ones are externally visible. The functional specification describes the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages. The product description defines the TSF to a level of detail such that the TSF can be generated without further design decisions.
M.TRACE	The developer provides correspondence mapping such that the security functionality detailed in the TOE functional specification is upwards traceable to the ST and downwards traceable to the TOE high-level design.
M.DOCS	Documentation is provided to the administrators that describe the administrative functions, describe how to administer the TOE in a secure manner, contain warnings about functions and privileges, describe assumptions regarding user behavior relevant to the secure operation of the TOE, describe all security parameters under the control of the administrator, describe each type of security relevant event relative to the administrative functions that need to be performed, and describe all security requirements for the IT environment that are relevant to the administrator. This guidance document lists all assumptions about the intended environment, all requirements for external security measures, and identifies all possible modes of operation of the TOE.
M.DEVSEC	The development security documentation provided describes the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
M.FLAW	Procedures are documented for accepting and acting upon user reports of security flaws and request for corrections to those flaws.
M.LIFE	A life-cycle model is used to develop and maintain the TOE. Documentation is provided that describes this model.

M.TEST	A correctly configured TOE is tested to confirm the TOE operates as specified. Documentation is provided to the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification. Test documentation is provided, which includes test plans, test procedure descriptions, expected results, and results from testing.
M.VULN	Documentation is provided that performs a strength of TOE security function analysis on specific mechanisms in the TOE. Documentation is provided that shows obvious ways that a user could violate the TSP, and that these vulnerabilities cannot be exploited in the intended environment.

7 RATIONALE

This section provides the rationale for the selection of the IT security requirements, objectives, assumptions, and threats. In particular, it shows that the IT security requirements are suitable to meet the security objectives, which in turn are shown to be suitable to cover all aspects of the TOE security environment.

7.1 Rationale for IT Security Objectives

This section provides a rationale for the existence of each assumption, threat, and policy statement that compose the STAT® Scanner Security Target. Table 7-1 Security Environment vs. Objectives demonstrates the mapping between the assumptions, threats, and polices to the security objectives is complete. Table 7-2 Security Objectives Rationale discusses the coverage for each assumption, threat, and policy.

Table 7-1 Security Environment vs. Objectives

	O.PROTCT	O.IDACTS	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	O.INSTAL	O.PHYCAL	O.CREDEN	O.PERSON	O.INTROP
A.ACCESS														X
A.DYNMIC													X	X
A.ITSYSCOR														X
A.ASCOPE														X
A.PROTCT											X			
A.LOCATE											X			
A.MANAGE													X	
A.NOEVIL										X	X	X		
A.NOTRUST											X	X		
T.COMINT	X			X	X			X						
T.COMDIS	X			X	X				X					
T.LOSSOF	X			X	X			X						
T.NOHALT		X		X	X									
T.PRIVIL	X			X	X									
T.IMPCON			X	X	X					X				
T.INFLUX						X								
T.FACCNT							X							
T.SCNCFG		X												
T.SCNMLC		X												
T.SCNVUL		X												
P.DETECT		X					X							
P.MANAGE	X		X	X	X					X		X	X	

	O.PROTCT	O.IDACTS	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	O.INSTAL	O.PHYCAL	O.CREDEN	O.PERSON	O.INTROP
P.ACCESS	X			X	X									
P.ACCACT					X		X							
P.INTEGR								X						
P.PROTCT						X					X			

Table 7-2 Security Objectives Rationale

A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions
	The O.INTROP objective ensures the TOE has the needed access.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
	The O.INTROP objective ensures the TOE has the proper access to the IT System. The O.PERSON objective ensures that the TOE will be managed appropriately.
A.ITSYSCOR	The TOE depends on the correct functioning of the IT System including: a. Domain Controller, b. Unix system security access components, c. Windows® system security access components, and, d. Network infrastructure and mapping.
	The O.INTROP objective ensures that the TOE can gain the necessary access to the IT System it is monitoring and acquire truthful data from its scan of the system.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.
	The O.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

	The O.PHYCAL provides for the physical protection of the TOE hardware and software.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
	The O.PHYCAL provides for the physical protection of the TOE.
A.MANAGE	There will be one or more individuals familiar with the software and technology comprising the TOE assigned to manage the TOE and the security of the information it contains.
	The O.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
	The O.INSTAL objective ensures that the TOE is properly installed and operated and the O.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The O.CREDEN objective supports this assumption by requiring protection of all authentication data
A.NOTRST	The TOE can only be accessed by authorized users.
	The O.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The O.CREDEN objective supports this assumption by requiring protection of all authentication data.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected by the TOE by bypassing a security mechanism.
	The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be modified. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.COMDIS	An unauthorized user may attempt to disclose the data collected by the TOE by bypassing a security mechanism.

	The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.EXPORT objective ensures that confidentiality of TOE data will be maintained. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected by the TOE.
	The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be deleted. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the STAT® Scanner‘s collection functionality by halting execution of the TOE.
	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.IDACTS objective addresses this threat by requiring the TOE to collect all events, including those attempts to halt the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

	The O.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
	The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.
	The O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.
T.SCNCFG	Improper security configuration settings may exist in the IT System the TOE monitors.
	The O.IDACTS objective counters this threat by requiring the TOE collect and store static configuration information that might be indicative of a configuration setting change
T.SCNMLC	Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.
	The O.IDACTS objective counters this threat by requiring the TOE collect and store static configuration information that might be indicative of malicious code.
T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors.
	The O.IDACTS objective counters this threat by requiring the TOE collect and store static configuration information that might be indicative of a vulnerability.
P.DETECT	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System must be collected.

	The O.AUDITS and O.IDACTS objectives address this policy by requiring collection of audit and STAT® Scanner data.
P.MANAGE	The TOE shall only be managed by authorized users.
	The O.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The O.INSTAL objective supports the O.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective addresses this policy by providing TOE self-protection.
P.ACCESS	All data collected by the TOE shall only be used for authorized purposes.
	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this policy by providing TOE self-protection.
P.ACCACT	Users of the TOE shall be accountable for their actions within the IDS.
	The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated.
P.INTGTY	Data collected by the TOE shall be protected from modification.
	The O.INTEGR objective ensures the protection of data from modification
P. PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of collection activities.

	The O.OFLOWS objective counters this policy by requiring the TOE handle disruptions. The O.PHYCAL objective protects the TOE from unauthorized physical modifications.

7.2 Rationale for Functional Security Requirements

This section demonstrates that the functional components described within this ST provide complete coverage of the defined security objectives. The mapping of components to security objectives is depicted in Table 7-3 Requirements vs. Objectives Mapping. Table 7-4 Evidence of Coverage for Security Objectives discusses the evidence of coverage for objective by the security functions.

Table 7-3 Requirements vs. Objectives Mapping

	O.PROTCT	O.IDACTS	O.EADMIN	O.IDAUTH	O.ACCESS	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT
FAU_GEN.1							X		
FAU_SAR.1			X						
FAU_SAR.2				X	X				
FAU_SAR.3			X						
FAU_SEL.1			X				X		
FAU_STG.2	X			X	X	X		X	
FAU_STG.4						X	X		
FIA_AFL.1	X			X	X				
FIA_UAU.1				X	X				
FIA_ATD.1				X					
FIA_UID.1				X	X				
FMT_MOF.1	X			X	X				
FMT_MTD.1	X			X	X			X	
FMT_SMR.1				X					
FPT_ITA.1									X
FPT_ITC.1								X	X
FPT_ITI.1								X	X
FPT_RVM.1	X		X	X			X	X	
FPT_SEP.1	X		X	X			X	X	
FPT_STM.1							X		
IDS_SCN.1		X							
IDS_RDR.1			X	X	X				
IDS_STG.1	X			X	X	X		X	
IDS_STG.2				X		X			

The following discussion provides detailed evidence of coverage for each security objective.

Table 7-4 Evidence of Coverage for Security Objectives

O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
	The TSF must address failures in authentication, this is provided by Windows® through the Winlogon process. Winlogon requires a correctly spelled password in order to grant an identified subject access to the system [FIA_AFL.1]. The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of audit storage exhaustion, failure [FAU_STG.2]. The STAT® Scanner is required to protect the data collected from an IT System from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure [IDS_STG.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the STAT® Scanner may query and add STAT® Scanner and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1].
O.IDACTS	The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.
	The Scanner is required to collect and store static configuration information of an IT System [IDS_SCN.1].
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
	The TOE must provide the ability to review and manage the audit trail of a Scanner [FAU_SAR.1, FAU_SAR.3, FAU_SEL.1]. The Scanner must provide the ability for authorized administrators to view the Scanner data collected from an IT System [IDS_RDR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1].

O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	The TSF must address failures in authentication, this is provided by Windows® through the Winlogon process. Winlogon requires a correctly spelled password in order to grant an identified subject access to the system [FIA_AFL.1]. The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The audit data of STAT® Scanner is restricted to administrators, who may select from vulnerability assessment, execution tracing, or STAT® Scanner configuration audit data. The Scanner is required to restrict the review of collected Scanner data to those granted with explicit read-access [IDS_RDR.1]. The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of audit storage exhaustion, failure [FAU_STG.2]. The Scanner is required to protect the Scanner data collected from an IT System from any modification and unauthorized deletion [IDS_STG.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the Scanner may query and add Scanner and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1].
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
	The TSF must address failures in authentication, this is provided by Windows® through the Winlogon process. Winlogon requires a correctly spelled password in order to grant an identified subject access to the system [FIA_AFL.1]. The authorized STAT® Scanner user may review all available audit data. The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The Scanner is required to restrict the review of collected Scanner data to those granted with explicit read-access [IDS_RDR.1]. The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of audit storage exhaustion, failure [FAU_STG.2]. The Scanner is required to protect the Scanner data collected from an IT System from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure [IDS_STG.1]. Security attributes of subjects used

	to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the Scanner may query and add Scanner and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1].
O.OFLOWS	The TOE must appropriately handle potential audit and Scanner data storage overflows.
	The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of audit storage exhaustion, failure [FAU_STG.2]. The TOE must prevent the loss of audit data in the event the IT audit trail is full [FAU_STG.4]. The Scanner is required to protect the Scanner data collected from an IT System from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure [IDS_STG.1]. The Scanner must prevent the loss of audit data in the event the IT audit trail is full [IDS_STG.2].
O.AUDITS	The TOE must record audit records for data accesses and use of the Scanner functions.
	Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The TOE must provide the capability to select which security-relevant events to audit [FAU.SEL.1]. The TOE must prevent the loss of collected data in the event the IT audit trail is full [FAU_STG.4]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1]. Time stamps associated with an audit record must be reliable [FPT_STM.1].
O.INTEGR	The TOE must ensure the integrity of all audit and Scanner data.

	The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of audit storage exhaustion, failure [FAU_STG.2]. The Scanner is required to protect the Scanner data collected from an IT System from any modification and unauthorized deletion [IDS_STG.1]. Only authorized administrators of the Scanner may query or add audit and Scanner data [FMT_MTD.1]. The Scanner must protect the collected data from modification and ensure its integrity when the data is transmitted to another IT product [FPT_ITC.1, FPT_ITI.1]. The TOE must ensure that all functions that protect the data are not bypassed [FPT_RVM.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1].
O.EXPORT	When the TOE makes its Scanner data available to other IDS components; the TOE will ensure the confidentiality of the Scanner data.
	The TOE must make the collected data available to other IT products [FPT_ITA.1]. The TOE must protect the collected data from modification and ensure its integrity when the data is transmitted to another IT product [FPT_ITC.1, FPT_ITI.1].

7.3 Rationale for Explicitly Stated Requirements

A family of IDS requirements was created to specifically address the data collected and analyzed by an IDS. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of IDS data and provide for requirements about collecting, reviewing and managing the data. These requirements have no dependencies since the stated requirements embody all the necessary security functions.

7.4 Rationale for Strength of Function

The TOE minimum strength of function is SOF-basic. The evaluated TOE is intended to operate in commercial, Government and military low robustness environments processing unclassified information. This security function is in turn consistent with the security objectives described in section 4.

7.5 Rationale for Assurance Requirements

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the STAT® Scanner may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the STAT® Scanner will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The nature of this STAT® Scanner product, and the fact that Harris releases monthly updates of the product to customers, requires a higher level of assurance over the development process than is required by EAL2. In order to provide higher assurance over these monthly product changes, the following assurance augmentations are required: ACM_CAP.4, ACM_SCP.1, ALC_DVS.1, ALC_FLR.3, ALC_LCD.1, AVA_MSU.1.

7.6 Rationale for Satisfying All Dependencies

This ST addresses and satisfies all security functional requirement dependencies outlined in the Common Criteria for the Intrusion Detection System Scanner Protection Profile. Table 7-5 Requirement Dependencies lists each requirement from the Intrusion Detection System Scanner Protection Profile with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 7-5 Requirement Dependencies

Functional Component	Dependency	Included
FAU_GEN.1	FPT_STM.1	YES
FAU_SAR.1	FAU_GEN.1	YES
FAU_SAR.2	FAU_SAR.1	YES
FAU_SAR.3	FAU_SAR.1	YES
FAU_SEL.1	FAU_GEN.1 & FMT_MTD.1	YES
FAU_STG.2	FAU_GEN.1	YES
FAU_STG.4	FAU_STG.2 CC shows FAU_STG.1	YES
FIA_AFL.1	FIA_UAU.1	YES
FIA_ATD.1	-	YES
FIA_UAU.1	FIA_UID.1	YES

Functional Component	Dependency	Included
FIA_UID.1	-	YES
FMT_MOF.1	FMT_SMR.1	YES
FMT_MTD.1	FMT_SMR.1	YES
FMT_SMR.1	FIA_UID.1	YES
FPT_ITA.1	-	YES
FPT_ITC.1	-	YES
FPT_ITI.1	-	YES
FPT_RVM.1	-	YES
FPT_SEP.1	-	YES
FPT_STM.1	-	YES
IDS_SCN.1	-	YES
IDS_RDR.1	-	YES
IDS_STG.1	-	YES
IDS_STG.2	-	YES
ACM_CAP.4	ACM_SCP.1 ALC_DVS.1	YES
ACM_SCP.1	ACM_CAP.3	YES
ADO_DEL.1	-	YES
ADO_IGS.1	AGD_ADM.1	YES
ADV_FSP.1	ADV_RCR.1	YES
ADV_HLD.1	ADV_FSP.1 & ADV_RCR.1	YES
ADV_RCR.1	-	YES
AGD_ADM.1	ADV_FSP.1	YES
AGD_USR.1	ADV_FSP.1	YES
ALC_DVS.1	-	YES
ALC_FLR.3	-	YES
ALC_LCD.1	-	YES
ATE_COV.1	ADV_FSP.1 and ATE_FUN.1	YES
ATE_FUN.1	-	YES
ATE_IND.2	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, and ATE_FUN.1	YES
AVA_VLA.1	ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, and AGD_USR.1	YES
AVA_SOF.1	ADV_FSP.1 and ADV_HLD.1	YES
AVA_MSU.1	ADO_IGS.1, ADV_FSP.1,	YES

Functional Component	Dependency	Included
	AGD_ADM.1, and AGD_USR.1	

7.7 TOE Summary Specification Rationale

7.7.1 TOE Security Functions Rationale

Table 7-6 Requirements vs. Security Function Mapping maps the security functions to the security functional requirements. Table 7-7 Evidence of Requirements vs. Security Function Mapping discusses how each security functional requirement is addressed by the corresponding security functions.

Table 7-6 Requirements vs. Security Function Mapping

	F.AUTH	F.AUTHFAIL	F.AUDEVT	F.AUDINF	F.DATAREV	F. DATAPRO	F.ROLE	F.USER	F.TSFDATA	F.AVAIL	F.TRANS	F.NOBPASS	F.DOMN	F.TIME	F.SCANDATA	
FAU.GEN.1			X	X										X		
FAU_SAR.1					X											
FAU_SAR.2					X											
FAU_SAR.3					X											
FAU_SEL.1			X													
FAU_STG.2						X										
FAU_STG.4						X										
FIA_AFL.1		X														
FIA_UAU.1	X															
FIA_ATD.1								X								
FIA_UID.1	X															
FMT_MOF.1									X							
FMT_MTD.1									X							
FMT_SMR.1							X									
FPT_ITA.1										X						
FPT_ITC.1											X					
FPT_ITI.1											X					
FPT_RVM.1												X				
FPT_SEP.1													X			
FPT_STM.1														X		
IDS_SCN.1															X	
IDS_RDR.1					X											
IDS_STG.1						X										
IDS_STG.2						X										

Table 7-7 Evidence of Requirements vs. Security Function Mapping

FAU_GEN.1	Audit data generation
	F.AUDEVT, F.AUDINF and F.TIME combine to satisfy the requirement for generation of audit data for auditable events.
FAU_SAR.1	Audit review
	F.DATAREV satisfies the requirements for reviewing of audit data.

FAU_SAR.2	Restricted audit review
	F.DATAREV satisfies the requirements for restricting review of audit data.
FAU_SAR.3	Selectable audit review
	F.DATAREV satisfies the requirements for selecting the audit data to review.
FAU_SEL.1	Selective audit review
	F.AUDEVT satisfies the requirements for configuring auditable events.
FAU_STG.2	Guarantee of audit data availability
	F.DATAPRO satisfies the requirements for guaranteeing audit data availability.
FAU_STG.4	Prevention of audit data loss
	F.DATAPRO satisfies the requirements for prevention of audit data loss.
FIA_AFL.1	Authentication failure handling
	F.AUTHFAIL satisfies the requirements for handling authentication failure.
FIA_UAU.1	Timing of authentication
	F.AUTH satisfies the requirements for restricting capabilities before successful authentication.
FIA_ATD.1	User attribute definition
	F.USER satisfies the requirements for keeping security attributes of users.
FIA_UID.1	User identification
	F.AUTH satisfies the requirements for restricting capabilities before successful identification.
FMT_MOF.1	Management of security functions

	F.TSFDATA satisfies the requirements for managing the behavior of security functions.
FMT_MTD.1	Management of TSF data
	F.TSFDATA satisfies the requirements for managing the TSF data.
FMT_SMR.1	Security roles
	F.ROLE satisfies the requirements for maintaining security roles.
FPT_ITA.1	Inter-TSF availability
	F.AVAIL satisfies the requirements for ensuring the availability of audit and STAT® Scanner data to remote trusted IT products.
FPT_ITC.1	Inter-TSF confidentiality during transmission
	F.TRANS satisfies the requirements for confidentiality of TSF data during transmission.
FPT_ITI.1	Inter-TSF detection of modification during transmission
	F.TRANS satisfies the requirements for detecting modifications of the TSF data during transmission.
FPT_RVM.1	Non-bypassability of the TSP within the TOE
	F.NOBYPASS satisfies the requirements for ensuring that the TSF enforcement functions are non-bypassable.
FPT_SEP.1	TSF domain separation
	F.DOMN satisfies the requirements for ensuring the TSF maintains a separate domain.
FPT_STM.1	Reliable time stamps
	F.TIME satisfies the requirement for reliable time stamps.
IDS_SCN.1	STAT® Scanner data collection
	F.SCANDATA satisfies the requirement for collecting scanner data.

IDS_RDR.1	Restricted data review
	F.DATAREV satisfies the requirements restricting review of data.
IDS_STG.1	Guarantee of STAT® Scanner data availability
	F.DATAPRO satisfies the requirements for prevention of unauthorized data deletion.
IDS_STG.2	Prevention of scanner data loss
	F.DATAPRO satisfies the requirements for actions taken when storage capacity is reached.

7.7.2 TOE Assurance Measures Rationale

Table 7-8 Assurance Measures vs. Assurance Functions Mapping maps the assurance measures to the assurance requirements. Table 7-9 Evidence of Assurance Measures vs. Assurance Functions Mapping discusses how each assurance requirement is addressed by the corresponding assurance measure.

Table 7-8 Assurance Measures vs. Assurance Functions Mapping

	M.ID	M.CMLIST	M.SYSTEM	M.GETTOE	M.SETUP	M.SPEC	M.TRACE	M.DOCS	M.DEVSEC	M.FLAW	M.LIFE	M.TEST	M.VULN
ACM_CAP.4	X	X	X										
ACM_SCP.1		X											
ADO_DEL.1				X									
ADO_IGS.1					X								
ADV_FSP.1						X							
ADV_HLD.1						X							
ADV_RCR.1							X						
AGD_ADM.1								X					
AGD_USR.1								X					
ALC_DVS.1									X				
ALC_LCD.1											X		
ALC_FLR.3										X			
ATE_COV.1												X	
ATE_FUN.1												X	
ATE_IND.2												X	
AVA_SOF.1													X
AVA_VLA.1													X
AVA_MSU.1													X

Table 7-9 Evidence of Assurance Measures vs. Assurance Functions Mapping

ACM_CAP.4	Generation support and acceptance procedures
	M.ID, M.CMLIST, and M.SYSTEM satisfy the requirements for supporting the generation of the TOE and providing acceptance procedures.
ACM_SCP.1	TOE CM coverage
	M.CMLIST satisfies the requirements for providing CM documentation.
ADO_DEL.1	Delivery procedures
	M.GETTOE satisfies the requirements for documenting delivery procedures.

ADO_IGS.1	Installation, generation, and start-up procedures
	M.SETUP satisfies the requirements for documenting procedures for secure installation, generation, and start-up procedures for the TOE.
ADV_FSP.1	Informal functional specification
	M.SPEC satisfies the requirements for providing a functional specification.
ADV_HLD.1	Descriptive high-level design
	M.SPEC satisfies the requirements for providing the high-level design of the TSF.
ADV_RCR.1	Informal correspondence demonstration
	M.TRACE satisfies the requirements for providing an information correspondence demonstration.
AGD_ADM.1	Administrator guidance
	M.DOCS satisfies the requirements for providing administrator guidance.
AGD_USR.1	User guidance
	M.DOCS satisfies the requirements for providing user guidance.
ALC_DVS.1	Identification of security measures
	M.DEVSEC satisfies the requirements for producing development security documentation.
ALC_LCD.1	Developer defined life-cycle model
	M.LIFE satisfies the requirements for documenting the established life-cycle model.
ALC_FLR.3	Systematic flaw remediation
	M.FLAW satisfies the requirements for documenting the procedures for flaw remediation.
ATE_COV.1	Evidence of coverage

	M.TEST satisfies the requirements for providing evidence of test coverage.
ATE_FUN.1	Functional testing
	M.TEST satisfies the requirements for documenting the results of the functional testing.
ATE_IND.2	Independent testing -sample
	M.TEST satisfies the requirements for providing the TOE for testing.
AVA_SOF.1	Strength of TOE security function evaluation
	M.VULN satisfies the requirements for providing strength of function claims for mechanisms.
AVA_VLA.1	Developer vulnerability analysis
	M.VULN satisfies the requirements for analyzing the TOE for vulnerabilities.
AVA_MSU.1	Examination of guidance
	M.VULN satisfies the requirements for providing guidance documentation.