Enterasys Networks, Inc.
Dragon Intrusion Defense System Version 7.2.3 Running on Dragon Appliances

Security Target

Document Version 2.0

Prepared for:

Enterasys Networks, Inc.
50 Minuteman Road
Andover, MA 01810
Tel: (978) 684-1000
Sales: (877) 801-7082

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
Phone: (703) 267-6050
Fax: (703) 267-6810

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2005-08-05	Adam O'Brien	Initial version.
0.2	2006-01-30	Elizabeth Goff	First EORs.
0.3	2006-02-14	Elizabeth Goff	Addressed miscellaneous lab feedback.
0.4	2006-02-16	Elizabeth Goff	Addressed miscellaneous lab feedback.
0.5	2006-02-16	Elizabeth Goff	Addressed miscellaneous lab feedback.
0.6	2006-02-17	Elizabeth Goff, Nathan Lee	Corrected misidentification of several Environmental Objectives.
0.7	2006-03-20	Elizabeth Goff	Updated documentation identification.
0.8	2006-07-30	Christie Kummers	Updated Physical TOE Boundary Diagram
0.9	2007-02-05	Christie Kummers	Updated SFRs.
0.91	2007-03-23	Christie Kummers	Updated SFRs and version number. Updated Section 8.7.2 to include ALC_FLR.2. Updated Table 9 with the correct Administrative Guide documents.
1.0	2007-05-21	Christie Kummers	Updated Table 3 – Auditable Events, Table 4 – Access control matrix for FMT_MTD.1, FMT_MTD.1(3), Section 6.1.1.
1.1	2007-06-29	Christie Kummers	Removed PP Conformance and updated the ST accordingly.
1.2	2007-07-27	Nathan Lee, Christie Kummers	Updated to address OR 6.
1.3	2007-08-02	Christie Kummers, Nathan Lee	Updated to address OR 6.
1.4	2007-09-05	Nathan Lee	Updated TOE version number to 7.2.3, miscellaneous cosmetic fixes.
1.5	2008-01-24	Nathan Lee	Corrected inconsistency in IDS_SDC.1.
1.6	2008-04-08	Nathan Lee	Corrected other inconsistencies in IDS_SDC.1.
1.7	2008-04-18	Nathan Lee	Miscellaneous corrections to prepare for testing.
1.8	2008-05-30	Nathan Lee	Updates SFRs based on lab feedback.
1.9	2008-07-10	Nathan Lee	Updated lists of supported OS'.
2.0	2008-10-06	Nathan Lee	Updated to address CSEC verdicts.

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), ST conventions, ST conformance claims, and the ST organization. The Target of Evaluation is the Enterasys Dragon Intrusion Defense System Version 7.2.3 Running on Dragon Appliances, and will hereafter be referred to as the TOE throughout this document. The TOE is an intrusion detection system coupled with intrusion prevention capabilities. It uses scanners and sensors to collect information about target systems and/or networks, and an analyzer component to support interpretation of the data and initiate actions in response to its findings.

1.1 Purpose

This ST contains the following sections to provide mapping of the Security Environment to the Security Requirements that the TOE meets in order to remove, diminish or mitigate the defined threats:

- Security Target Introduction (Section 1) – Provides a brief summary of the content of the ST and describes the organization of other sections of this document.
- TOE Description (Section 2) – Provides an overview of the TOE security functions and describes the physical and logical boundaries for the TOE.
- Security Environment (Section 3) – Describes the threats, assumptions, and the Organizational Security Policy that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Security Requirements (Section 5) – Presents the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE and by the TOE's environment.
- TOE Summary Specification (Section 6) – Describes the security functions provided by the TOE to satisfy the security requirements and objectives.
- Protection Profile Claims (Section 7) – Provides the identification of the ST Protection Profile claims as well as a justification to support such claims.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability.
- Acronyms and Terminology (Section 9) – Defines the acronyms and terms used within this ST.

1.2 Security Target, TOE and CC Identification and Conformance

Table 1 – ST, TOE, and CC Identification and Conformance

ST Title	Enterasys Networks, Inc. Dragon Intrusion Defense System Version 7.2.3 Running on Dragon Appliances Security Target
ST Version	Version 2.0
Author	Corsec Security, Inc. Elizabeth Goff, Christie Kummers, Nathan Lee
TOE Identification	Enterasys Dragon Intrusion Defense System Version 7.2.3 Running on Dragon Appliances

Common (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 2.2 Revision 326, December 2004 (aligned with ISO[1]15408:2004); Parts 2 and 3 Interpretations from the Interpreted CEM as of August 15th, 2005 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None. (Modeled after the *Intrusion Detection System System Protection Profile, Version 1.5, March 9, 2005*)
Evaluation Assurance Level (EAL)	EAL2 augmented with ALC_FLR.2
Keywords	Intrusion Defense, Intrusion Prevention, Network Monitoring, Intrusion Detection, Dragon

1.3 Conventions, Acronyms, and Terminology

1.3.1 Conventions

The following conventions have been applied in this document.

The CC permits four functional component operations—assignment, refinement, selection, and iteration —to be performed on functional requirements. The following conventions have been used to indicate the use of these operations.

- assignment: allows the specification of an identified parameter. Indicated with bold text and italics where further operations have been made by the Security Target author;
- refinement: allows the addition of details. Indicated with bold text and italics if further operations have been made by the Security Target author;
- selection: allows the specification of one or more elements from a list. Indicated with underlined text; and
- iteration: allows a component to be used more than once with varying operations. Iterations are identified by appending a number in parenthesis following the component title. For example, FAU_GEN.1(1) Audit Data Generation would be the first iteration and FAU_GEN.1(2) Audit Data Generation would be the second iteration.

In addition, this ST has explicitly stated requirements. These new requirements are indicated in bold text and contain the text “EXP” in the title.

1.3.2 Acronyms and Terminology

The acronyms and terms used within this ST are described in Section 9 – “Acronyms and Terminology”

[1] International Organization for Standardization (ISO)

2 TOE Description

This section provides a general overview of the product as an aid to understanding the capabilities and security functionality offered. The TOE description provides a context for the evaluation by outlining the physical components and logical features which are included in the TOE and describing the evaluated configuration

2.1 Product Type

The Dragon Intrusion Defense System is an intrusion detection system coupled with intrusion prevention capability. This class of product performs network and host based intrusion detection. Additionally, these types of products manage and monitor routers, switches, firewalls, applications, and web servers. These systems use agents to detect and respond to suspicious activity based on collected forensic data to determine the impact of network attacks. Intrusion prevention capabilities allow systems to drop offending packets and neutralize threats after an identified attack by terminating an attacker's session or establishing firewall access policies.

2.2 Product Description

The product is an intrusion detection and prevention system which uses sensors to collect information about target systems and networks. The system contains an analyzer component to support interpretation of the data and initiate actions in response to its findings. The Dragon Intrusion Defense System contains the following five main components:

- Dragon Enterprise Management Server (EMS)
- Dragon Enterprise Management Client (Client)
- Dragon Network Sensor
- Dragon Security Module on N-Series Switch
- Dragon Host Sensor

These five product components are deployed as shown in Figure 1.

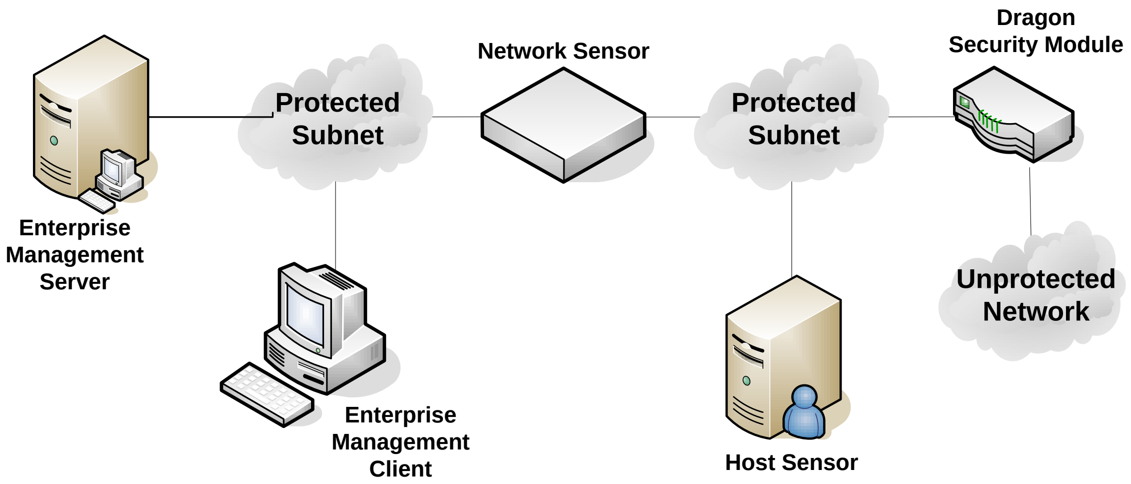

Figure 1 – Deployment Configuration of the TOE

Dragon Enterprise Management Server (EMS):

The EMS is the central management server for the Dragon Intrusion Defense System. The EMS provides the Host Sensor, Network Sensor, and Dragon Security Module components with the most current policies for enforcement.

The enforcement policies are created on, stored, and deployed from the EMS. To ensure that these policies are enforced based on up-to-date signatures, the EMS automatically downloads updated Intrusion Detection System (IDS) signatures over the internet and distribute them to all sensor components. All sensor components report event information back to the EMS to be consolidated, stored and analyzed for trends. Additionally, the EMS maintains the list of users and user privileges for all system components. This allows the system's user management to be centralized.

The EMS grants permission to authorized users to view events generated by the sensors via a web-based reporting interface called "Dragon Reporting" (called the "Session Management" Interface in the supporting Common Criteria architecture documentation). "Dragon Reporting" displays reports stored on the EMS and provides summary information of attacks, activity graphs, summary of rebuilt network sessions, and analysis of event trends. The "Dragon Reporting" interface is comprised of four consoles available through a web browser: the Forensics Console, Realtime Console, Trending Console and Executive Reporting Console.

Dragon Enterprise Management Client (Client):

The Enterprise Management Client is a Java client that can be used on both Windows and Linux operating systems to gain remote access to the full management features of the EMS. The Enterprise Management Client provides a graphical user interfaces to manage users and their associated roles, Host and Network Sensors, policies, and alarms associated with specific events. In addition to changing a components' configuration it provides a means to view the status of all deployed sensors.

Dragon Network Sensor:

The first of three sensor components in the Enterasys Intrusion Defense System, the Dragon Network Sensor is a network intrusion detection system (NIDS). The Dragon Network Sensor is deployed between subnets and collects network packets and analyzes them for suspicious activities. It can detect anomalies such as malformed network protocol headers and potentially malicious port scans. The Dragon Network Sensor can also provide SNMP alerts, enforcement of event-based policy, and reconstruction of packet and session traffic. It can also match network patterns that may indicate probes, attacks, compromises, and other types of network abuse.

In addition to typical intrusion detection capabilities, the Dragon Network Sensor employs active response techniques to block detected attacks. The Dragon Network Sensor can respond by terminating any sessions found to be potentially hostile and can reconfigure firewalls, switches, and routers to block attacks in-progress. The Dragon Network Sensor can also analyze network-based attacks using forensic tools that capture packets and record complete session information. If an attack is suspected, the Dragon Network Sensor can take protective action. For example, the Dragon Network Sensor can create access control lists blocking certain IP addresses.

The Dragon Network Sensor is a software package that can be installed on any of the following Dragon Network Sensor Appliances:

- DSNSA7-FE100-TX,
- DSNSA7-GE250-TX/SX,
- DSNSA7-GE500-TX/SX,
- DSNSA7-GIG-TX/SX,

Dragon Security Module:

The second of three sensor components, the Dragon Security Module is also a NIDS. The Dragon Security Module is a Linux-based blade, which provides NIDS functionality for a Matrix N-Series Enterasys Switch. The Security Module is similar to the Dragon Network Sensor and provides similar functionality. Dragon Security Modules can be managed from the EMS in the same fashion as Network Sensors.

Dragon Host Sensor:

The third of the three sensor components, the Dragon Host Sensor is a software host-based Intrusion Detection System also offering intrusion prevention functionality. The Dragon Host Sensor can operate on any host running

Windows 2000/XP/2003/Vista, Sparc Solaris, AIX, HPUX, and the following Linux Distributions: Red Hat Enterprise Linux, Fedora Core, SuSE, CentOS, and Slackware. It can be installed on any system capable of running these operating systems.

2.3 TOE Boundaries and Scope

This section will address which physical and logical components of the Dragon Intrusion Defense System are included in the TOE.

2.3.1 Physical Boundary

Figure 2 illustrates the physical boundary and scope of the Dragon Intrusion Defense System and ties together the components of the TOE and the constituents of the TOE Environment. The Enterasys Networks Dragon Intrusion Defense System Version 7.2 running on Dragon Appliances will hereafter be referred to as the TOE throughout this document.

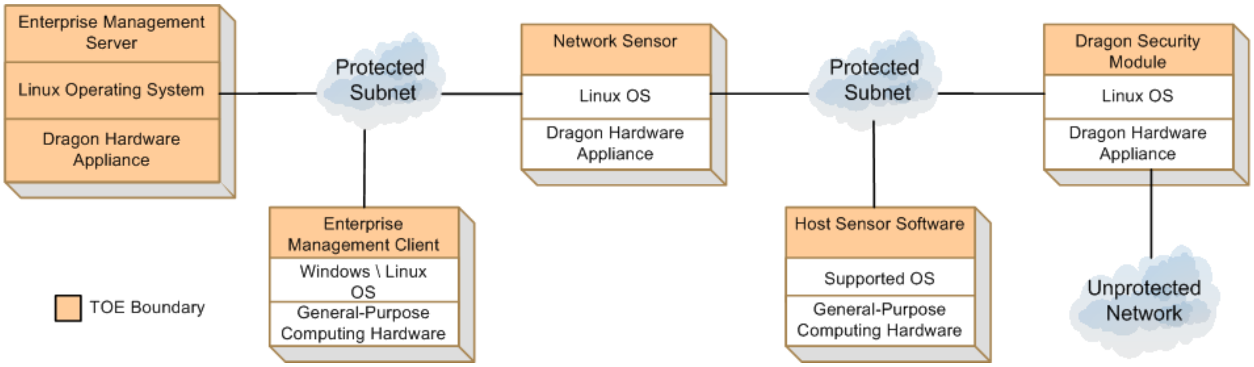
Enterprise Management Server
Linux Operating System
Dragon Hardware Appliance
Protected Subnet
Network Sensor
Linux OS
Dragon Hardware Appliance
Protected Subnet
Dragon Security Module
Linux OS
Dragon Hardware Appliance
Enterprise Management Client
Windows \ Linux OS
General-Purpose Computing Hardware
Host Sensor Software
Supported OS
General-Purpose Computing Hardware
Unprotected Network
TOE Boundary

Figure 2 – Physical TOE Boundary

The physical components that comprise the TOE are:

- Dragon Enterprise Management Server: The Dragon EMS is a dedicated appliance running the Enterasys Networks modified version of Linux.
- Dragon Network Sensor software component is part of the TOE but the Linux kernel operating system and underlying hardware are excluded.
- Dragon Host Sensor software component is part of the TOE but the operating system and underlying hardware are excluded.
- Dragon Security Module software component is part of the TOE but the Linux-based Matrix N-Series blade, the blade operating system, and the switch on which it runs are excluded.
- Dragon Enterprise Management Client software component is part of the TOE but the operating system and underlying hardware are excluded.

2.3.2 Logical Boundary

The Logical Boundaries of the TOE are embodied in the security functions that it implements. These TOE security functions are usefully grouped under the following Security Function Classes:

- Security Audit
- Identification and Authentication
- Security Management
- TOE Self Protection
- IDS Component Requirements

Each of these security functions are discussed below.

2.3.2.1 Security Audit

The Security Audit function incorporates the generation, storage and viewing of audit records. The TOE generates two types of audit data; network events which contain IDS information received from sensors and audit records which contain information regarding the administration and management of the EMS. As a result of network and host scanning, each sensor collects security event data. The data collected is sent to the EMS for central storage and viewing. Audit records are also generated on the EMS and stored locally with no direct TOE administrator access. TOE users assigned to appropriate roles may read audit records but have no write access. When the audit logs have reached their maximum capacity an alert will be generated and the TOE will prevent auditable actions except those taken by authorized administrators. Authorized users can view and sort the audit records via the Enterprise Management Client, and view, sort, or delete audit records via the Command Line Interface (CLI) of the EMS.

2.3.2.2 Identification and Authentication

All identification and authentication for the TOE occurs on the EMS. TOE users are not able to log into the Host Sensor, Network Sensor or Dragon Security Module in the evaluated configuration; therefore those components do not perform any identification and authentication. Identification and authentication for users logging in via the EMS Client or web-based reporting interface is based on user attributes. Each user has a username, password and one or more roles assigned to them. The TOE ensures that users are authenticated prior to any use of the TOE functions, and user authentication is performed using a unique username and password combination. TOE users are allowed three unsuccessful login attempts before the account is locked out for thirty minutes.

2.3.2.3 Security Management

The TOE manages the Host and Network Sensor components, Dragon Security Modules, users, IDS signatures, and reporting data. Management of the sensor components includes reporting the status of the sensors and allowing security policies to be centrally created and deployed. Management and configuration of the TOE is performed by an administrator who has been assigned to one or more of the applicable roles via the Enterprise Management Client.

2.3.2.4 TOE Self Protection

The TOE protects itself by providing a domain for its own execution that cannot be accessed by untrusted subjects, and by ensuring that the TSFs cannot be bypassed. A TOE execution domain is provided by a combination of physical protection of the TOE, a TSF that prevents access by unauthorized users, and lack of visibility to non-TOE devices, users, or entities on the systems being monitored. Non-bypassability of the TSFs is provided by preventing unauthorized users to access the TOE and by role enforcement. The TOE provides a reliable time stamp mechanism for its own use.

2.3.2.5 IDS Component Requirements

The TOE includes sensors to collect and analyze IDS data. The Dragon Host Sensor provides data collection and analysis capabilities by scanning selected entities. The Dragon Host Sensor monitors system attributes to detect potential attacks. The Dragon Network Sensor and Dragon Security Module provide data collection and data analysis using network traffic from remote networks. Network events detected by the sensors are sent to the EMS which can generate alerts for selected users.

2.3.3 Excluded Functionality

The following features and functionality are excluded in the Common Criteria Evaluated Configuration of the TOE:

- Remote administration via Secure Shell (SSH) on the Dragon Network Sensors
- Command Line Interfaces on the Dragon Network Sensor

- Management of the EMS via SNMP
- Intrusion Protection Functionality

3 Security Environment

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be deployed. Section 3.1 provides assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects. Section 3.2 lists the known and presumed threats countered by either the TOE or by the security environment. Section 3.3 presents the Organizational Security Policies.

3.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

3.1.1 Intended Usage Assumptions

A.ACCESS The TOE has access to all the IT[2] 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.ASCOPE The TOE is appropriately scalable to the IT System the TOE monitors.

3.1.2 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.

3.1.3 Personnel Assumptions

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

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.

3.2 Threats to Security

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

3.2.1 TOE Threats

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

[2] Information Technology (IT)

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

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

T.NOHALT An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions 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 the TOE may go undetected.

3.2.2 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.

T.FALACT The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.

T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

T.MISUSE Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.

T.INADVE Inadvertent activity and access may occur on an IT System the TOE monitors.

T.MISACT Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

3.3 Organization Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. This section identifies the organizational security policies applicable to the TOE.

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 or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.

P.ANALYZ Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

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

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

P.ACCACT Users of the TOE shall be accountable for their actions through auditing all authorized and unauthorized access to the TOE.

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

P. PROTCT The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

4 Security Objectives

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.

4.1 Information Technology (IT) Security Objectives

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.IDSCAN 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.

O.IDSENS The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.

O.IDANLZ The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).

O.RESPON The TOE must respond appropriately to analytical conclusions.

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 prior to allowing access to TOE functions and data.

O.OFLOWS The TOE must appropriately handle potential audit and System data storage overflows.

O.AUDITS The TOE must record audit records for authorized and unauthorized access to the TOE.

O.INTEGR The TOE must ensure the integrity of all audit and System data.

O.EXPORT When any IDS component makes its data available to another IDS components, the TOE will ensure the confidentiality of the System data.

4.2 Security Objectives for the Environment

The TOE's operating environment must satisfy the following objectives.

4.2.1 Non-IT Objectives

These objectives do not levy any IT requirements but are satisfied by procedural or administrative measures.

OE.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.

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

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

OE.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.

OE.INTROP The TOE is interoperable with the IT System it monitors.

4.2.2 IT Objectives

OE.TIME The IT Environment will provide reliable timestamps to the TOE

OE.PROTECT The IT environment will protect itself and the TOE from external interference or tampering.

5 Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE as well as Security Functional Requirements met by the TOE IT environment. These requirements are presented following the conventions identified in Section 1.3.1.

5.1 TOE Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the TOE. This section organizes the SFRs by CC class. Table 2 identifies all SFRs implemented by the TOE.

Table 2 – TOE Security Functional Requirements

SFR ID	Description
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_SAR.3	Selectable audit review
FAU_STG.2	Guarantees of audit data availability
FAU_STG.4	Prevention of audit data loss
FIA_ATD.1	User attribute definition
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FMT_MOF.1	Management of security functions behaviour
FMT_MTD.1(1)	Management of TSF data
FMT_MTD.1(2)	Management of TSF data
FMT_MTD.1(3)	Management of TSF data
FMT_MTD.1(4)	Management of TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_RVM.1(1)	Non-bypassability of the TSP
FPT_SEP.1(1)	TSF domain separation
FPT_STM.1(1)	Reliable time stamps
IDS_SDC.1	System Data Collection
IDS_ANL.1	Analyzer analysis
IDS_RCT.1	Analyzer react
IDS_RDR.1	Restricted Data Review
IDS_STG.1	Guarantee of System Data Availability
IDS_STG.2	Prevention of System Data Loss

Section 5.1 contains the functional components from the Common Criteria (CC) Part 2 with the operations completed. For the conventions used in performing CC operations please refer to Section 1.3.1.

5.1.1 Class FAU: Security Audit

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 not specified level of audit; and

c) ***The auditable events specified in Table 3***.

Table 3 – Auditable Events

Auditable Event	Details	Associated SFRs
Reading of information from the audit records	When audit records are viewed through the EMS Client	FAU_SAR.1 FAU_SAR.2
Unsuccessful attempts to read information from the audit records	When audit records are viewed through the EMS Client	
Successful use of the authentication mechanism	When the authentication mechanism is used, the following information is recorded on the user interfaces: • Enterprise Management Client Interface: User identity • Command Line Interface: User identity, User location • “Dragon Reporting” web-based Interface: User identity, User location	FIA_UAU.2
Unsuccessful use of the authentication mechanism	When the authentication mechanism is used, the following information is recorded on the user interfaces: • Enterprise Management Client Interface: User identity • Command Line Interface: User identity, User location • “Dragon Reporting” web-based Interface: User identity, User location	
Successful use of the user identification mechanism	When the identification mechanism is used, the following information is recorded on the user interfaces: • Enterprise Management Client Interface: User identity • Command Line Interface: User identity, User location • “Dragon Reporting” web-based Interface: User identity, User location	FIA_UID.2
Unsuccessful use of the user identification mechanism	When the identification mechanism is used, the following information is recorded on the user interfaces: • Enterprise Management Client Interface: User identity • Command Line Interface: User identity, User location • “Dragon Reporting” web-based Interface: User location	

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 3 – Auditable Events***.

FAU_SAR.1 Audit review

FAU_SAR.1.1

The TSF shall provide ***the authorised System administrators*** with the capability to read ***all audit information*** from the audit records.

FAU_SAR.1.2

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

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.3 Selectable audit review

FAU_SAR.3.1

The TSF shall provide the ability to perform <u>sorting</u> of audit data based on ***date and time, subject identity, type of event, and success or failure of related event***.

FAU_STG.2 Guarantees of audit data availability

FAU_STG.2.1

The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.2.2

The TSF shall be able to <u>prevent</u> modifications to the audit records.

FAU_STG.2.3

The TSF shall ensure that ***the previously recorded*** audit records will be maintained when the following conditions occur: <u>audit storage exhaustion</u>.

FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1

The TSF shall ignore auditable events and send an alarm if the audit trail is full.

5.1.2 Class FIA: Identification and Authentication

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) ***Authorisations; and***

d) ***No other attributes***.

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1

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

FIA_UID.2 User identification before any action

FIA_UID.2.1

The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.3 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1

The TSF shall restrict the ability to <u>modify the behaviour</u> of the functions ***of System data collection, analysis and reaction*** to ***authorised System administrators***.

Application Note: FMT_MTD.1 has been iterated to specify one action on one type of data in order to clarify which roles may perform each action. Table 4 – Access control matrix for FMT_MTD.1 presents an access matrix specifying the abilities of the different roles on the different types of data as specified in FMT_MTD.1(1) – FMT_MTD.1(4). The different types of data are listed in the top row, the roles are listed in the left column, and the body contains the different rights (query(Q), add(A), or modify(M)) each role has on each data type.

Data type Role			TOE data					
	System data	Audit data	Deploy Configuration	Change / Commit Configuration	View Configuration	View Topology	Reporting GUI	Manage Users
DragonSuperAdmin	Q	Q	Q, M	Q,M	Q	Q	Q	Q, M
DragonAdmin			Q, M	Q, M	Q	Q		
DragonReports	Q						Q	
DragonDeployAdmin			Q, M		Q	Q		
DragonCommitAdmin				Q, M	Q	Q		
DragonViewConfigAdmin					Q	Q		
DragonViewAdmin						Q		
DragonUserAdmin								Q, M
Authorized system administrator		Q						

Table 4 – Access control matrix for FMT_MTD.1

FMT_MTD.1(1) Management of TSF data

FMT_MTD.1.1

The TSF shall restrict the ability to <u>query</u> the ***System data*** to ***DragonSuperAdmin, DragonReports.***

FMT_MTD.1(2) Management of TSF data

FMT_MTD.1.1

The TSF shall restrict the ability to <u>query</u> the ***audit data*** to ***DragonSuperAdmin, the authorized system administrator.***

FMT_MTD.1(3) Management of TSF data

FMT_MTD.1.1

The TSF shall restrict the ability to query ***all TOE data not specified in FMT_MTD.1(1) and FMT_MTD.1(2)*** to ***DragonSuperAdmin, DragonAdmin, DragonDeployAdmin, DragonCommitAdmin, DragonViewConfigAdmin, DragonViewAdmin, DragonUserAdmin according to the matrix given in Table 4.***

FMT_MTD.1(4) Management of TSF data

FMT_MTD.1.1

The TSF shall restrict the ability to modify ***all TOE data not specified in FMT_MTD.1(1) and FMT_MTD.1(2)*** to ***DragonSuperAdmin, DragonAdmin, DragonDeployAdmin, DragonCommitAdmin, DragonUserAdmin according to the matrix given in Table 4.***

FMT_SMF.1 Specification of management functions

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions: ***TSF data management and security function management***.

FMT_SMR.1 Security roles

FMT_SMR.1.1

The TSF shall maintain the following roles: ***authorised System administrator, and DragonDeployAdmin, DragonCommitAdmin, DragonViewConfigAdmin, DragonViewAdmin, DragonReports, DragonUserAdmin, DragonSuperAdmin, DragonAdmin.***

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Application Note: authorised System administrator is a role provided and maintained by the underlying EMS Operating System.

5.1.4 Class FPT: Protection of the TSF

FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1

The TSF shall protect TSF data from <u>disclosure, modification</u> whe*n* it is transmitted between separate parts of the TOE.

FPT_RVM.1(1) Non-bypassability of the TSP

FPT_RVM.1.1(1)

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

FPT_SEP.1(1) TSF domain separation

FPT_SEP.1.1(1)

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

FPT_SEP.1.2(1)

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

FPT_STM.1(1) Reliable time stamps

FPT_STM.1.1(1)

The ***EMS*** shall be able to provide reliable time stamps for its own use.

5.1.5 Class IDS: IDS Component Requirements (IDS)

IDS_SDC.1 System Data Collection (EXP)

IDS_SDC.1.1

The System shall be able to collect the following information from the targeted IT System resource(s):

a) The Events specified in the Event column of Table 5 – IDS Events (EXP)

IDS_SDC.1.2

At a minimum, the System 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 – IDS Events. (EXP)

Table 5 – IDS Events

Component	Event	Details
IDS_SDC.1	Start-up and shutdown	none
IDS_SDC.1	Data modifications	Object IDS, requested access, destination address
IDS_SDC.1	Network traffic	Protocol, source address, destination address
IDS_SDC.1	Security configuration changes	Destination address
IDS_SDC.1	Data introduction (into existing files resulting in file-size increase)	Object IDS, location of object, destination address
IDS_SDC.1	Detected malicious code	Location, identification of code
IDS_SDC.1	Service configuration	Service identification (name or port)
IDS_SDC.1	Accountability policy configuration	Accountability policy configuration parameters

IDS_ANL.1 Analyser analysis (EXP)

IDS_ANL.1.1

The System shall perform the following analysis function(s) on all IDS data received:

a) signature; and

b) no other events. (EXP)

IDS_ANL.1.2

The System shall record within each analytical result at least the following information:

a. Date and time of the result, type of result, identification of data source; and

b. no other events. (EXP)

IDS_RCT.1 Analyser react (EXP)

IDS_RCT.1.1

The System shall send an alarm to the authorized administrator(s) via email and create a System data record when an intrusion is detected. (EXP)

IDS_RDR.1 Restricted Data Review (EXP)

IDS_RDR.1.1

The System shall provide DragonSuperAdmin, DragonReports with the capability to read all system data from the System data. (EXP)

IDS_RDR.1.2

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

IDS_RDR.1.3

The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access. (EXP)

IDS_STG.1 Guarantee of System Data Availability (EXP)

IDS_STG.1.1

The System shall protect the stored System data from unauthorised deletion. (EXP)

IDS_ STG.1.2

The System shall protect the stored System data from modification. (EXP)

IDS_ STG.1.3

The System shall ensure that the previously recorded System data will be maintained when the following conditions occur: System data storage exhaustion. (EXP)

IDS_STG.2 Prevention of System data loss (EXP)

IDS_STG.2.1

The System shall ignore System data and send an alarm if the storage capacity has been reached. (EXP)

5.2 Security Requirements for the Environment

This section specifies the SFRs for the TOE environment. This section organizes the SFRs by CC class. Table 6 identifies all SFRs implemented by the TOE environment and indicates the ST operations performed on each requirement.

Table 6 – TOE Environment SFRs

SFR ID	Description
FPT_RVM.1(2)	Non-bypassability of the TSP
FPT_SEP.1(2)	TSF domain separation
FPT_STM.1(2)	Reliable time stamps

5.2.1 Class FPT: Protection of the TSF

FPT_RVM.1(2) Non-bypassability of the TSP

FPT_RVM.1.1(2)

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

FPT_SEP.1(2) TSF domain separation

FPT_SEP.1.1(2)

The ***environment*** shall maintain a security domain for ***the Dragon Host Sensor's, Dragon Network Sensor's, and Dragon Security Module's*** execution that protects them from interference and tampering by untrusted subjects.

FPT_SEP.1.2(2)

The ***environment*** shall enforce separation between the security domains of subjects in the TSC.

FPT_STM.1(2) Reliable time stamps

FPT_STM.1.1(2)

The ***environment of the Dragon Host Sensor*** shall be able to provide reliable time stamps for ***the Dragon Host Sensor's, Dragon Network Sensor's, and Dragon Security Module's*** use.

5.3 Assurance Requirements

This chapter defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.2. Table 7 – Assurance Components summarizes the components.

Table 7 – Assurance Components

Assurance Requirements	
Class ACM: Configuration management	ACM_CAP.2 Configuration items
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

Assurance Requirements	
	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_FLR.2 Flaw reporting procedures
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

6 TOE Summary Specification

This section presents information to detail how the TOE meets the functional and assurance requirements described in previous sections of this ST.

6.1 TOE Security Functions

Each of the security function descriptions is organized by the security requirements corresponding to the security function. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions are suitable to satisfy the necessary requirements.

Table 8 – Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.2	Guarantees of audit data availability
	FAU_STG.4	Prevention of audit data loss
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of security functions
	FMT_MTD.1(1)	Management of TSF data
	FMT_MTD.1(2)	Management of TSF data
	FMT_MTD.1(3)	Management of TSF data
	FMT_MTD.1(4)	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_RVM.1(1)	Non-bypassability of the TSP
	FPT_SEP.1(1)	TSF domain separation
	FPT_STM.1(1)	Reliable time stamps
IDS Component Requirements	IDS_SDC.1	System Data Collection
	IDS_ANL.1	Analyzer analysis
	IDS_RCT.1	Analyzer react
	IDS_RDR.1	Restricted Data Review
	IDS_STG.1	Guarantee of System Data Availability
	IDS_STG.2	Prevention of System data loss

6.1.1 Security Audit

The TOE generates two types of audit data; audit records which contain information regarding the administration of the TOE, and IDS/IPS event records which contain IDS/IPS information received from the sensors. This security function addresses the generation, storage and viewing of audit records. The separate TOE security function called "IDS Component Requirements" covers the generation, storage, and viewing of the IDS event records. IDS Event Records are discussed in Section 6.1.5.

The TOE administrators interact with the TOE through the EMS CLI and the Enterprise Management Client and the EMS Session Management (commonly called "Dragon Reporting") interfaces. The Enterprise Management Client and the EMS "Dragon Reporting" interfaces are mechanisms for interacting with the EMS and as such actions made through either interface are recorded in the EMS. The TOE creates an audit record when a TOE administrator causes any of the events in Table 3 to occur. Audit records generated in the EMS are stored within a datastore (composed of log files) which is a subcomponent of the EMS. Audit records include the date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event. When the audit event relates to authentication or identification of users, the identity of the user responsible for the event is also recorded (except on the "Dragon Reporting" interface). TOE administrators do not have direct access to the datastore. TOE administrators can read audit records only through the EMS CLI and Enterprise Management Client interfaces, and only when authenticated as described below. TOE administrators are never given write access to the audit records. When the capacity of the datastore has been reached, the TOE stops writing auditable events and an email alert is sent to a selected TOE administrator.

Only TOE authorised System administrators can read the audit data. The Enterasys Networks modified Linux operating system and the Enterprise Management Client provides the necessary tools to view and sort the audit records. When viewing the logs through the Enterasys Networks modified Linux operating system, it is possible to sort the audit records based on the following fields:

- Time and date of the occurrence
- User
- Type of event
- Success of failure of the related event.

When viewing the logs through the Enterprise Management Client, it is possible to sort the audit records based on date.

Security Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.2, FAU_STG.4

6.1.2 Identification and Authentication

This section discusses the TOE controls on user access and the user attributes used by the TOE to make access control decisions. TOE administrators can properly access the TOE in three ways; via the Enterprise Management Client (a Graphical User Interface or GUI), the EMS Command Line Interface (CLI), or via the "Dragon Reporting" web page consoles. The TOE administrators do not directly access the other TOE components. For all methods of access the identification and authentication mechanism is provided by the Enterprise Management Server. The EMS stores a username, a hashed password (i.e. authentication data), and the roles associated with the administrator (i.e. authorizations), for each TOE administrator. A administrator is authenticated when the hash of the password that has been entered matches the stored hashed password. Prior to identification and authentication of an administrator via the GUI, EMS CLI, or web interface, no actions are allowed on behalf of the administrator. Any user attempting to interact with the TOE is presented only with a login screen until successful identification and authentication is completed. Roles are assigned to administrators when the administrator account is created. Login is not permitted if there is no associated role for the administrator.

TOE Security Functional Requirements Satisfied: FIA_ATD.1, FIA_UAU.2, FIA_UID.2

6.1.3 Security Management

This section discusses the TOE's role definition and role management functionalities. The TOE maintains nine (9) roles which are identified in FMT_SMR.1. The roles determine an administrator's level of access to security management functions provided by the TOE. These security management functions are the management of all audit and event records, management of access control, and management of IDS functions used to collect, react to and analyze data. An administrator can be assigned one or more roles from the list of available roles.

User attempts to manage TOE security functionality and change, query, modify, or delete security attributes originate at the Enterprise Management Client or the "Dragon Reporting" interface. All requests for services from either of these interfaces are passed to the EMS, which mediates the access control to those functions. The EMS makes the access control decision by comparing the administrator's role and the privilege requirement for the type of request made.

TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_SMF.1, FMT_SMR.1

6.1.4 Protection of the TSF

The TOE provides several mechanisms for protecting its security functions. The TOE protects all TSF data from disclosure when it is transmitted to separate parts of the TOE by using either SSL (using the Advanced Encryption Algorithm (AES) for encryption) or direct encryption with AES. The sensors communicate with the EMS via the EMS dedicated management network port. All traffic between the sensors and the EMS is encrypted with AES. The sensors and EMS are also configured to only accept traffic from specific IP addresses and are configured with a shared secret to validate their identity. The Enterprise Management Client and the "Dragon Reporting" web-based interface use SSL (using AES for encryption) to communicate with the EMS.

The TOE consists of five architecturally separate components that are listed below. The five physical TOE components all ensure that security mechanisms cannot be bypassed; however, all TOE components except the EMS rely on the TOE environment to enforce domain separation.

- Dragon Enterprise Management Server
- Dragon Enterprise Management Client
- Dragon Network Sensor
- Dragon Host Sensor
- Dragon Security Module

The EMS is a software application which runs on a dedicated appliance with a customized Linux operating system. This component of the TOE enforces domain separation and ensures that the security mechanisms cannot be bypassed. The security mechanisms cannot be bypassed because all management and configuration functions of the TOE are carried out only by Authorized TOE Users. All management and configuration operations are conducted in the context of an associated management session. This management session is established only after an administrator has successfully authenticated. Sessions ensure that all future communications within the context of that session are logically linked to the original authentication. All management and configuration operations are checked for conformance to the granted level of access and rejected if non-conformant. The management session is destroyed when the corresponding TOE User logs out of that session. No management functions can be executed by a non-authenticated administrator. This ensures that security protection enforcement functions are invoked and succeed before each function within the TSF scope of control is allowed to proceed. These mechanisms are linked deeply into the operating system (OS) access control, process management, and TCP session management mechanisms. These mechanisms operate correctly because they are protected by the Domain Separation mechanisms.

Protection of the TOE from physical tampering is ensured by its environment. It is the responsibility of the administrator to assure that the physical connections made to the TOE remain intact and unmodified. The EMS is self contained; the hardware and firmware provide all the services necessary to implement the EMS supported TSFs. No general purpose operating system, programming interfaces or external disk storage is provided. The EMS maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects. The TOE's protected domain includes the preloaded TSF Software on the appliance. The TSF Software is compiled and built as a single, monolithic entity and is loaded onto the appliance. The provided administrator interfaces restrict the administrator to a specific set of commands; therefore the software files on the EMS cannot be modified without violating the physical security of the EMS. The underlying assumption regarding the operation of the EMS is that it is maintained in a physically secure environment. Using kernel/user mode switching, the Linux OS controls the execution of each process and ensures that all the information used for management purposes is protected from direct access by any other process. Furthermore, in order to ensure the correct execution of each process, the OS protects each process's private information (executable code, data, and stack) from uncontrolled interferences from other processes. These features ensure that the TSF maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

The Dragon Enterprise Management Client does not directly enforce any security mechanisms; therefore non-bypassability is not applicable. The Dragon Enterprise Management Client operates in its own domain of execution provided by the underlying operating system and hardware (the environment), which is not part of the TOE.

The Dragon Network Sensor contains a network interface in promiscuous mode i.e. it receives and analyses all network traffic. The tight control of the ability to make configuration changes on the EMS ensures that the sensor cannot be disabled by an attacker. The logic of event processing on the Dragon Network Sensor ensures that all activities indicative of intrusions are reported to the EMS. Therefore this sensor will detect and react to all appropriate network traffic and is non-bypassable. The Dragon Network Sensor operates in its own domain of execution provided by the underlying firmware and hardware (the environment), which is not part of the TOE.

The Dragon Host Sensor monitors operating system events by redirecting kernel events to custom processes which detect activities indicative of intrusion and then passes the events back to OS control for execution. Since it operates at such a low-level within the monitored operating system its functionality cannot be bypassed. The Dragon Host Sensor operates in its own domain of execution provided by the underlying operating system and hardware (the environment), which is not part of the TOE.

The Dragon Security Module has a network interface operating, in promiscuous mode; i.e. it receives and analyzes all network traffic. The tight control of the ability to make configuration changes on the EMS ensures that the sensor cannot be disabled by a hostile user. The simple logic of event processing ensures that all activities indicative of intrusions are reported to the EMS. Therefore this sensor will detect and react to all appropriate network traffic and is non-bypassable. The Dragon Security Module operates in its own domain of execution provided by the underlying firmware and hardware (the environment), which is not part of the TOE.

The Dragon Enterprise Management Client provides reliable timestamps for its own use and for the use of the Dragon Network Sensor and the Dragon Security Module. The Dragon Network Sensor and the Dragon Security Module receive time information via the Network Time Protocol. The Dragon Host Sensor takes timestamps from the environment, specifically the operating system it is monitoring.

TOE Security Functional Requirements Satisfied: FPT_ITT.1, FPT_RVM.1(1), FPT_SEP.1(1), FPT_STM.1(1)

6.1.5 IDS Component Requirements

The TOE provides intrusion detection functions that include collection of data from sensor and scanner functions as well as analysis functions found within the sensors themselves and the Enterprise Management System.

The Dragon Host Sensor is used to monitor the host it is installed on and is capable of monitoring both host traffic and host system files. The Dragon Network Sensor and the Dragon Security Module can detect suspicious events by monitoring network traffic from configured networks. The sensors collect IDS event records and transmit them to the EMS. The EMS provides functionality to view collected IDS event records as well as to determine summary information.

6.1.5.1 Data Collection and Analysis by the Host Sensor

The Dragon Host Sensor performs scanning activities by monitoring designated data and files on the host system. The Host Sensor can continuously monitor the system or can be configured to run at scheduled intervals. The Host Sensor collects information about data accesses and security configuration changes. Three specific techniques are used to monitor the host: scanning, integrity, and signature based analysis techniques.

Scanning activities include the following:

- File attributes: File attributes are monitored and events are generated when values are changed from the administrator-established known "good" state. File permissions, file user ownership, file group ownership, inode values, file deletion, file truncation, file growth, and modification time changes are all monitored.
- Linux TCP/UDP Service: On Linux platforms, specific TCP and UDP services can be monitored to generate events as services are started or existing services terminate.
- Integrity analysis activities include the following:
  - File MD5: Files are monitored for modification by periodically recalculating a file's MD5 checksum, and comparing it to the stored checksum. Events are logged when changes are detected.
- Linux Kernel: When the Dragon Host Sensor detects that any system calls or kernel interrupts have been "hooked" and generates events if hooking is detected.
- Signature-based analysis includes the following:
  - File content: The content of log files can be scanned and if specified signature patterns exist, and alarms can be generated used to alert a specified TOE administrator.

6.1.5.2 Data Collection and Analysis by the Dragon Network Sensor and Dragon Security Module

The Dragon Network Sensor and Dragon Security Module collect network packets and analyze them for suspicious activities. Configuration files control the type of network traffic to be collected and where the results are to be recorded. It can detect anomalies such as malformed network protocol headers and potentially malicious port scans. The network sensor components can also provide enforcement of event-based policies and reconstruction of packet and session traffic. The network sensor components process reconstructed packets as if the original packet had not been fragmented. In much the same way, the network sensor components can piece together network packets to monitor portions of sessions. It can also match network patterns that may indicate probes, attacks, compromises, and other types of network abuse.

The network sensor components provide several different signature-based analysis methods. They include the following:

- Resource signatures: This usage signature assumes that any attack or probe which attempts to exploit a particular network resource will use that resource at some time. The network sensor components maintain a list of specific unwanted actions associated with a specific resource. When an unwanted action occurs on the associated resource an event is recorded.
- Suspicious signatures: These signatures focus on data that should not be present in a specific type of network session. For example, "CGI-BIN" attacks are designed to run commands on target machines. As these commands or programs should not occur in normal traffic, identifying them may indicate a web attack in progress.
- Server messages: The server messages analysis method monitors the informational and error messages from a server for common indicators of an attack. Many times it is easier to look for attacks in the return traffic from a server. For example, a server message that an account was closed because of 10 unsuccessful login attempts could be evidence of an attack.
- Indirect signatures: These are network patterns that may indirectly indicate some form of network misuse or system compromise. The network sensor components scan a set of patterns of defined network events that are typically observed during various attacks.

When any of these signature analysis methods identify a possible intrusion an IDS event record is sent to the EMS. Recorded events are sorted into event groups, which are assigned event types:

• Suspicious:	Traffic that may have potential security ramifications
• Probe:	Attempts to map out a network but not exploit it
• Attacks:	Actual known attacks with intent to compromise a server
• Compromise:	Evidence of a successful attack
• Vulnerability:	Evidence of a known vulnerability
• Trojan:	Evidence of an active Trojan horse network program
• Virus:	Evidence of an active network virus

The network sensor components can include raw data (packets) as well as header and event information and the results of analysis of the data. Recorded network events include the date and time of the event, event type, subject identity, protocol, source address, and destination address. Analysis data includes the date and time of the result, type of result, identification of data source. The raw packets that triggered the analysis are also included.

6.1.5.3 Data Collection and Analysis by the EMS

The EMS stores all the IDS event records generated by the sensors components of the TOE in a central location for analysis and viewing. The EMS stores the IDS event records in a dedicated database. TOE administrators do not have direct access to this database. TOE administrators in appropriate roles can read IDS event records through the EMS, but no write access is granted. The default capacity of the database is 8 gigabytes. Once this is reached the Sensors will stop listening for events, the EMS will ignore system data, and an alert is sent to a selected TOE administrator. Alerts are generated by the Alarmtool agent. Alarmtool can be configured through the Enterprise Management Client and allows administrators to be notified when a specific system event has occurred or when the sensors detect an anomaly. The type of notification and conditions for administrator notification are customizable and extendable. The notification of the administrator can take many forms. These include email, log files, the UNIX syslog facility, and external program execution of the administrators' choice. Notifications can be constrained via time periods, filters, event groups and the distinction between real time and summarized events.

The EMS Real Time console and the Forensics console process event data from sensors and display them in a human readable format. They provide tools for sorting, scoring, and listing events. The two consoles have similar functionality. The Real Time console gets information from the real-time shell while the Forensics console gets information from the event database. The EMS Trending console processes collected event data from the event database and utilizes SQL queries to build web displays of IP addresses, events, or searching for unique event entries. For each query, the top seven matches over the selected time range are displayed.

TOE Security Functional Requirements Satisfied: IDS_SDC.1, IDS_ANL.1, IDS_RCT.1, IDS_RDR.1, IDS_STG.1, IDS_STG.2

6.2 TOE Security Assurance Measures

EAL2 augmented was chosen to provide a basic level of independently assured security. This section of the Security Target maps the assurance requirements of the TOE for a CC EAL2 augmented level of assurance to the assurance measures used for the development and maintenance of the TOE. The following table provides a mapping of the appropriate documentation to the TOE assurance requirements.

Table 9 – Assurance Measures Mapping to TOE Security Assurance Requirements (SARs)

Assurance Component	Assurance Measure
ACM_CAP.2	9034256 Enterasys Dragon Intrusion Defense System Version 7.2.3 Running on Dragon Appliances – Configuration Management
ADO_DEL.1	9034257 Enterasys Dragon Intrusion Defense System Version 7.2.3 Running on Dragon Appliances – Secure Delivery

Assurance Component	Assurance Measure
ADO_IGS.1	Dragon Intrusion Defense System Appliance Quick Start, Dragon Intrusion Defense System Installation Guide, Dragon Intrusion Defense System Rack Mount Guide
ADV_FSP.1	9034258 Enterasys Dragon Intrusion Defense System Version 7.2.3 Running on Dragon Appliances – TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
ADV_HLD.1	9034258 Enterasys Dragon Intrusion Defense System Version 7.2.3 Running on Dragon Appliances – TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
ADV_RCR.1	9034258 Enterasys Dragon Intrusion Defense System Version 7.2.3 Running on Dragon Appliances – TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
AGD_ADM.1	Enterasys Dragon Intrusion Defense System Configuration Guide P/N 9033999-10 Enterasys Networks, Inc. Dragon Intrusion Defense System Version 7.2.3 Running on Dragon Appliances Administrative Guide Supplement
AGD_USR.1	Enterasys Dragon Intrusion Defense System Configuration Guide P/N 9033999-10
ALC_FLR.2	9034259 Enterasys Dragon Intrusion Defense System Version 7.2.3 Running on Dragon Appliances – Flaw Remediation
ATE_COV.1	9034260 Enterasys Dragon Intrusion Defense System Version 7.2.3 Running on Dragon Appliances – Functional Tests and Coverage
ATE_FUN.1	9034260 Enterasys Dragon Intrusion Defense System Version 7.2.3 Running on Dragon Appliances – Functional Tests and Coverage
ATE_IND.2	Provided by laboratory evaluation
AVA_SOF.1	9034261 Enterasys Dragon Intrusion Defense System Version 7.2.3 Running on Dragon Appliances – Vulnerability Assessment
AVA_VLA.1	9034261 Enterasys Dragon Intrusion Defense System Version 7.2.3 Running on Dragon Appliances – Vulnerability Assessment

6.2.1 ACM_CAP.2: Configuration Management Document

The Configuration Management document provides a description of the various tools used to control the configuration items and how they are used internally at Enterasys. This document provides a complete configuration item list and a unique referencing scheme for each configuration item. Additionally, the configuration management system is described including procedures that are used by developers to control and track changes that are made to the TOE. The documentation further details the TOE configuration items that are controlled by the configuration management system.

6.2.2 ADO_DEL.1: Delivery and Operation Document

The Delivery and Operation document provides a description of the secure delivery procedures implemented by Enterasys to protect against TOE modification during product delivery. The Installation Documentation provided by Enterasys details the procedures for installing the TOE and placing the TOE in a secure state offering the same protection properties as the master copy of the TOE. The Installation Documentation provides guidance to the TOE Users(s) on configuring the TOE and how they affect the TSF.

6.2.3 ADO_IGS.1: Installation Guidance, AGD_ADM.1: Administrator Guidance, AGD_USR.1: User Guidance

The installation guidance document provides the procedures necessary for the secure installation, generation, and start-up of the TOE for administrators and users of the TOE.

The administrator guidance documentation provides detailed procedures for the administration of the TOE and description of the security functions provided by the TOE.

The User Guidance documentation provided directs users on how to operate the TOE in a secure manner. Additionally, User Guidance explains the user-visible security functions and how they need to be exercised.

6.2.4 ADV_FSP.1: Informal Functional Specification, ADV_HLD.1: High Level Design, ADV_RCR.1: Representation Correspondence.

The Enterasys design documentation consists of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and errors message for each external TSF interface.
- The High-Level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high-level design identifies the basic structure of the TSF, the major elements, a listing of all interfaces, and the purpose and method of use for each interface.
- The Representation Correspondence demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from the ST description to the High-Level Design.

6.2.5 ALC_FLR.2: Flaw reporting procedures

The Flaw Remediation document outlines the steps taken at Enterasys to capture, track and remove bugs. The documentation shows that all flaws are recorded and that the system tracks them to completion.

6.2.6 ATE_COV.1: Test Coverage Analysis, ATE_FUN.1: Functional Testing

There are a number of components that make up the Test documentation. The Coverage Analysis demonstrates that testing is performed against the functional specification. The Coverage Analysis demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which the TOE was tested. Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided in order to meet the assurance requirement Functional Testing.

6.2.7 AVA_VLA.1: Vulnerability Analysis, AVA_SOF.1: Strength of Function Analysis

A Vulnerability Assessment is provided to demonstrate ways in which an entity could violate the TSP and provide a list of identified vulnerabilities. Additionally, this document provides evidence of how the TOE is resistant to obvious attacks.

The Strength of TOE Security Function Analysis demonstrates the strength of the probabilistic or permutational mechanisms employed to provide security functions within the TOE and how they exceed the minimum SOF requirements.

7 Protection Profile Claims

This section provides the identification and justification for any Protection Profile conformance claims.

7.1 Protection Profile Reference

This Security Target does not claim conformance to any Protection Profile; however, this Security Target is modeled after the Intrusion Detection System System Protection Profile, Version 1.5, March 9, 2005.

8 Rationale

This section provides the rationale for the selection of the security requirements, objectives, assumptions, and threats. In particular, it shows that the 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.

8.1 Security Objectives Rationale

This section provides a rationale for the existence of each assumption, threat, and policy statement that compose the Security Target. Table 10 demonstrates the mapping between the assumptions, threats, and polices to the security objectives is complete. The following discussion provides detailed evidence of coverage for each assumption, threat, and policy.

Table 10 – Relationship of Security Threats to Objectives

Objectives		TOE												Env.						
Threats, Assumptions		O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.PROTECT	OE.TIME
Assumptions	A.ACCESS																	✓		
	A.DYNMIC																✓	✓		
	A.ASCOPE																	✓		
	A.PROTCT														✓					
	A.LOCATE														✓					
	A.MANAGE																✓			
	A.NOEVIL													✓	✓	✓				
	A.NOTRUST														✓	✓				
Threats	T.COMINT	✓						✓	✓			✓							✓	
	T.COMDIS	✓						✓	✓				✓						✓	
	T.LOSSOF	✓						✓	✓			✓								
	T.NOHALT		✓	✓	✓			✓	✓											
	T.PRIVIL	✓						✓	✓											
	T.IMPCON						✓	✓	✓					✓						
	T.INFLUX									✓										
	T.FACCNT										✓									
	T.SCNCFG		✓																	
	T.SCNMLC		✓																	
	T.SCNVUL		✓																	
	T.FALACT					✓														
	T.FALREC				✓															
	T.FALASC				✓															

Objectives		TOE												Env.						
	T.MISUSE			✓																
	T.INADVE			✓																
	T.MISACT			✓																
OSPs	P.DETECT		✓	✓																✓
	P.ANALYZ				✓															
	P.MANAGE	✓					✓	✓	✓					✓		✓	✓			
	P.ACCESS	✓						✓	✓											
	P.ACCACT								✓		✓									✓
	P.INTGTY											✓								
	P.PROTCT									✓					✓				✓	

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

The OE.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 OE.INTROP objective ensures the TOE has the proper access to the IT System. The OE.PERSON objective ensures that the TOE will managed appropriately.

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

The OE.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 OE.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 OE.PHYCAL provides for the physical protection of the TOE.

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

The OE.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 OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.

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

The OE.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The OE.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 and produced 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. The OE.PROTECT objective supports the meeting of this policy by ensuring that the environment protects the TOE from bypass attacks.

T.COMDIS **An unauthorized user may attempt to disclose the data collected and produced 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. The OE.PROTECT objective supports the meeting of this policy by ensuring that the environment protects the TOE from bypass attacks.

T.LOSSOF **An unauthorized user may attempt to remove or destroy data collected and produced 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 System's collection and analysis functions 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.IDSCAN, O.IDSENS, and O.IDANLZ objectives address this threat by requiring the TOE to collect and analyze System data, which includes 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 OE.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 the TOE 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.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, 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.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, 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.IDSCAN objective counters this threat by requiring a TOE, which contains a Scanner, to collect and store static configuration information that might be indicative of a vulnerability.

T.FALACT **The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.**

The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.

T.FALREC **The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.**

The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source.

T.FALASC **The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.**

The O. IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.

T.MISUSE **Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.**

The O.IDSENS objective addresses this threat by requiring a TOE, that contains a Sensor, collect Sensor data.

T.INADVE **Inadvertent activity and access may occur on an IT System the TOE monitors.**

The O.IDSENS objective addresses this threat by requiring a TOE, that contains a Sensor, collect Sensor data.

T.MISACT **Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.**

The O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect Sensor data.

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 or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.**

The O.IDSENS and O.IDSCAN objectives address this policy by requiring collection of Sensor and Scanner data. Where required these objectives are supported by OE.TIME, the objective that the environment provide reliable timestamps.

P.ANALYZ **Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.**

The O.IDANLZ objective requires analytical processes be applied to data collected from Sensors and Scanners.

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

The OE.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 OE.INSTAL objective supports the OE.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 OE.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 and produced 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 by requiring the auditing of all authorized and unauthorized access to the TOE.**

The O.AUDITS objective implements this policy by requiring auditing of all accesses to the TOE. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. Where required these objectives are supported by OE.TIME.

P.INTGTY **Data collected and produced 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 TOE data and functions.**

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

OE.PROTECT objective supports the meeting of this policy by ensuring that the environment protects the TOE from external entities.

8.2 Security Functional Requirements Rationale

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

Table 11 – Relationship of Security Requirements to Objectives

Objectives		TOE												Env.	
Requirements		O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	OE.PROTECT	OE.TIME
TOE	FAU_GEN.1										✓				
	FAU_SAR.1						✓								
	FAU_SAR.2							✓	✓						
	FAU_SAR.3						✓								
	FAU_STG.2	✓						✓	✓	✓		✓			
	FAU_STG.4									✓	✓				
	FIA_UAU.2							✓	✓						
	FIA_ATD.1								✓						
	FIA_UID.2							✓	✓						
	FMT_MOF.1	✓						✓	✓						
	FMT_MTD.1(1)	✓						✓	✓			✓			
	FMT_MTD.1(2)	✓						✓	✓			✓			
	FMT_MTD.1(3)	✓						✓	✓			✓			
	FMT_MTD.1(4)	✓						✓	✓			✓			
	FMT_SMF.1	✓						✓	✓			✓			
	FMT_SMR.1								✓						
	FPT_ITT.1											✓	✓		
	FPT_RVM.1(1)	✓					✓		✓		✓	✓			
	FPT_SEP.1(1)	✓					✓		✓		✓	✓			
	FPT_STM.1(1)										✓				
	IDS_SDC.1		✓	✓											
	IDS_ANL.1				✓										
	IDS_RCT.1					✓									
	IDS_RDR.1						✓	✓	✓						
	IDS_STG.1	✓						✓	✓	✓		✓			
	IDS_STG.2									✓					

Objectives		TOE												Env.	
Env	FPT_RVM.1(2)													✓	
	FPT_SEP.1(2)													✓	
	FPT_STM.1(2)														✓

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

O.PROTCT **The TOE must protect itself from unauthorized modifications and access to its functions and 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 storage exhaustion, failure or attack [FAU_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. The TOE should provide facilities to enable the authorized user to manage the TOE [FMT_SMF.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 System may query System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4)]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1(1)]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1(1)].

O.IDSCAN **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.**

A System containing a Scanner is required to collect and store static configuration information of an IT System [IDS_SDC.1].

O.IDSENS **The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.**

A System containing a Sensor is required to collect events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets of an IT System [IDS_SDC.1].

O.IDANLZ **The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).**

The Analyzer is required to perform intrusion analysis and generate conclusions [IDS_ANL.1].

O.RESPON **The TOE must respond appropriately to analytical conclusions.**

The TOE is required to respond accordingly in the event an intrusion is detected [IDS_RCT.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 the System [FAU_SAR.1, FAU_SAR.3]. The System must provide the ability for authorized administrators to view all System data collected and produced [IDS_RDR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1(1)]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1(1)].

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

The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The System is required to restrict the review of System 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 storage exhaustion, failure or attack [FAU_STG.2]. The System is required to protect the System data 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.2, FIA_UAU.2]. The TOE should provide facilities to enable the authorized user to manage the TOE [FMT_SMF.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 System may query System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4).

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

The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. The TOE is required to protect the stored audit records from unauthorized deletion [FAU_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. Security attributes of subjects use 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.2, FIA_UAU.2]. The TOE should provide facilities to enable the authorized user to manage the TOE [FMT_SMF.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 System may query System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4)]. 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(1)]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1(1)].

O.OFLOWS **The TOE must appropriately handle potential audit and System 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 storage exhaustion, failure or attack [FAU_STG.2]. The TOE must prevent the loss of audit data in the event the its audit trail is full [FAU_STG.4]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. The System must prevent the loss of audit data in the event the its audit trail is full [IDS_STG.2].

O.AUDITS **The TOE must record audit records for authorized and unauthorized access to the TOE.**

Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The TOE must prevent the loss of collected data in the event the its 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(1)]. The TSF must be protected form interference that would prevent it from performing its functions [FPT_SEP.1(1)]. Time stamps associated with an audit record must be reliable [FPT_STM.1(1)].

O.INTEGR **The TOE must ensure the integrity of all audit and System 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 storage exhaustion, failure or attack [FAU_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.1]. The TOE should provide facilities to enable the authorized user to manage the TOE [FMT_SMF.1]. Only authorized administrators of the System may query audit and System data [FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4)]. The System must protect the collected data from modification and ensure its integrity when the data is transmitted to another IT product [FPT_ITT.1]. The TOE must ensure that all functions to protect the data are not bypassed [FPT_RVM.1(1)]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1(1)].

O.EXPORT **When any IDS component makes its data available to another IDS components, the TOE will ensure the confidentiality of the System data.**

The TOE must protect all data from modification and ensure its integrity when the data is transmitted to another IT product [FPT_ITT.1].

OE.TIME **The IT Environment will provide reliable timestamps to the TOE**

The IT environment of the Dragon Host Sensor is required to provide reliable timestamps to the Dragon Host sensor [FPT_STM.1(2)]

OE.PROTECT **The IT environment will protect itself and the TOE from external interference or tampering.**

The IT environment must ensure that all functions to protect the data are not bypassed [FPT_RVM.1(2)]. The IT environment must protect the TOE from interference that would prevent it from performing its functions [FPT_SEP.1(2)].

8.3 Security Assurance Requirements Rationale

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 System 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 System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer’s on-going flaw remediation processes.

8.4 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.

8.5 Rationale for Strength of Function

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

8.6 Dependency Rationale

This ST satisfies all the requirement dependencies of the Common Criteria. Table 12 Requirement Dependencies lists each requirement from the ST with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 12 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met
FAU_GEN.1	FPT_STM.1	✓
FAU_SAR.1	FAU_GEN.1	✓
FAU_SAR.2	FAU_SAR.1	✓
FAU_SAR.3	FAU_SAR.1	✓
FAU_STG.2	FAU_GEN.1	✓
FAU_STG.4	FAU_STG.2	✓
FIA_UAU.2	FIA_UID.1	✓ (FIA_UID.2 is hierarchical to FIA_UID.1)
FMT_MOF.1	FMT_SMF.1 and FMT_SMR.1	✓
FMT_MTD.1(1)	FMT_SMF.1 and FMT_SMR.1	✓
FMT_MTD.1(2)	FMT_SMF.1 and FMT_SMR.1	✓
FMT_MTD.1(3)	FMT_SMF.1 and FMT_SMR.1	✓
FMT_MTD.1(4)	FMT_SMF.1 and FMT_SMR.1	✓
FMT_SMR.1	FIA_UID.1	✓ (FIA_UID.2 is hierarchical to FIA_UID.1)

8.7 TOE Summary Specification Rationale

8.7.1 TOE Summary Specification Rationale for the Security Functional Requirements

Each subsection in the TOE Summary Specification (Section 6) describes a security function of the TOE. Each description is organized by set of requirements with rationale that indicates how these requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality. This section, in conjunction with the TOE Summary Specification section, provides evidence that the security functions are suitable to fulfill the TOE security requirements.

Table 13 identifies the relationship between security requirements and security functions, showing that all security requirements are addressed and all security functions are necessary (i.e., they correspond to at least one security requirement).

The only security mechanism that is realized by a probabilistic or permutational implementation is the password mechanism. For an analysis of the Strength of Function, refer to Strength of Function (SOF) Rationale section.

Table 13 – Mapping of Security Functional Requirements to TOE Security Functions

TOE Security Function	SFR	Rationale
Security Audit	FAU_GEN.1	The Security Audit TSF meets this requirement by providing an audit generation capability that records the necessary information about the required events as listed in Table 3.
	FAU_SAR.1	The Security Audit TSF meets this requirement by providing only authorized users with the ability to read and interpret all audit information from the audit records.
	FAU_SAR.2	
	FAU_SAR.3	The Security Audit TSF meets this requirement by providing authorized users with the ability to sort audit records for reading and interpretation.
	FAU_STG.2	The Security Audit TSF meets this requirement by protecting all audit records from unauthorized modification.
	FAU_STG.4	The Security Audit TSF meets this requirement by providing a mechanism for preventing certain auditable events to be written to the audit record when the audit trail is full.
Identification and Authentication	FIA_ATD.1	The Identification and Authentication TSF meets this requirement by ensuring that security attributes required to make identification and authentication decisions are maintained for TOE users.
	FIA_UAU.2	The Identification and Authentication TSF meets this requirement by requiring that TOE users must identify themselves and be authenticated before being allowed access to the TSF.
	FIA_UID.2	
Security Management	FMT_MOF.1	The Security Management TSF meets this requirement by restricting the ability to modify behaviour of the functions of System data collection, analysis, and reaction, to authorised System administrators..
	FMT_MTD.1(1)	The Security Management TSF meets this requirement by allowing only authorized users to query System data.
	FMT_MTD.1(2)	The Security Management TSF meets this requirement by allowing only authorized users to query audit data.
	FMT_MTD.1(3)	The Security Management TSF meets this requirement by allowing only authorized users to query all TOE data not specified in FMT_MTD.1(1) and FMT_MTD.1(2).
	FMT_MTD.1(4)	The Security Management TSF meets this requirement by allowing only authorized users to modify all TOE data not specified in FMT_MTD.1(1) and FMT_MTD.1(2).
	FMT_SMF.1	The Security Management TSF meets this requirement by providing specific management functions for administering the TOE.
	FMT_SMR.1	The Security Management TSF meets this requirement by maintaining the roles *authorised System administrator, DragonDeployAdmin, DragonCommitAdmin, DragonViewConfigAdmin, DragonViewAdmin, DragonReports, DragonUserAdmin, DragonSuperAdmin,* and *DragonAdmin*.
Protection of the TSF	FPT_ITT.1	The Protection of the TSF TSF meets this requirement by protecting the confidentiality and integrity of data flowing between physically distinct components of the TOE.
	FPT_RVM.1(1)	The Protection of the TSF TSF meets this requirement by ensuring that the TSF is not bypassable.

TOE Security Function	SFR	Rationale
	FPT_SEP.1(1)	The Protection of the TSF TSF meets this requirement by ensuring that the TOE has a separate domain of operation.
	FPT_STM.1(1)	The Protection of the TSF TSF meets this requirement by ensuring that the EMS provides reliable timestamps.
IDS Component Requirements	IDS_SDC.1	The IDS Component Requirements TSF meets this requirement by providing the capability to record necessary IDS data.
	IDS_ANL.1	The IDS Component Requirements TSF meets this requirement by providing a mechanism for the TOE to analyze all IDS data.
	IDS_RCT.1	The IDS Component Requirements TSF meets this requirement by providing a mechanism to alert the authorized administrator when an intrusion is detected.
	IDS_RDR.1	The IDS Component Requirements TSF meets this requirement by providing only authorized users with the ability to read and interpret all IDS data (system data).
	IDS_STG.1	The IDS Component Requirements TSF meets this requirement by protecting all IDS data (system data) from unauthorized modification.
	IDS_STG.2	The IDS Component Requirements TSF meets this requirement by providing a mechanism for ignoring IDS data and sending an alarm when the storage capacity is reached.

8.7.2 TOE Summary Specification Rationale for the Security Assurance Requirements

EAL2 augmented was chosen to provide a basic level of independently assured security. The chosen assurance level is consistent with the postulated threat environment.

8.7.2.1 Configuration Management

The Configuration Management documentation provides a description of tools used to control the configuration items and how they are used at Enterasys. The documentation provides a complete configuration item list and a unique reference for each item. Additionally, the configuration management system describes the procedures that are used by developers to control and track changes that are made to the TOE. The documentation further details the TOE configuration items that are controlled by the configuration management system.

Corresponding CC Assurance Components:

- Configuration Items

8.7.2.2 Delivery and Operation

The Delivery and Operation documentation provides a description of the secure delivery procedures implemented by Enterasys to protect against TOE modification during product delivery. The Installation Documentation provided by Enterasys details the procedures for installing the TOE and placing the TOE in a secure state. The Installation Documentation provides guidance to the administrators of the TOE regarding configuration parameters and how they affect the TSF.

Corresponding CC Assurance Components:

- Delivery Procedures
- Installation, Generation and Start-Up Procedures

8.7.2.3 Development

The Enterasys design documentation consists of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and errors message for each external TSF interface.
- The High-Level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high-level design identifies the basic structure of the TSF, the major elements, a listing of all interfaces, and the purpose and method of use for each interface.
- The Correspondence Analysis demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from the ST description to the High-Level Design.

Corresponding CC Assurance Components:

- Informal Functional Specification
- Descriptive High-Level Design
- Informal Representation Correspondence

8.7.2.4 Guidance Documentation

The Enterasys Guidance documentation provides administrator guidance on how to securely operate the TOE. The administrator Guidance provides descriptions of the security functions provided by the TOE. Additionally, it provides detailed accurate information for administration of the TOE in a secure manner and how to effectively use the TSF privileges and protective functions. Enterasys provides single versions of documents which address the administrator Guidance and User Guidance; there are not separate guidance documents specifically for non-administrator users of the TOE.

Corresponding CC Assurance Components:

- Administrator Guidance

8.7.2.5 Life Cycle Support

The Enterasys Life Cycle Support documentation describes the processes that Enterasys follows to identify, examine, track, and correct flaws (or “bugs”) that are found within the TOE. The documentation demonstrates that all discovered flaws are recorded and that the process ensures that flaws are tracked through their entire life cycle.

Corresponding CC Assurance Components:

- Flaw Reporting Procedures

8.7.2.6 Tests

Two components make up the Test documentation. The Coverage Analysis demonstrates the testing performed against the functional specification. The Coverage Analysis demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which the TOE was tested. Enterasys Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided.

Corresponding CC Assurance Components:

- Evidence of Coverage
- Functional Testing

8.7.2.7 Vulnerability and TOE Strength of Function Analyses

A Vulnerability Assessment is provided to demonstrate ways in which an entity could violate the TSP and provide a list of identified vulnerabilities. Additionally, the document provides evidence of how the TOE is resistant to obvious attacks. The Strength of TOE Security Function Analysis demonstrates the strength of the probabilistic or permutational mechanisms employed to provide security functions within the TOE and how they exceed the minimum SOF requirements.

Corresponding CC Assurance Components:

- Strength of TOE Security Function analysis
- Vulnerability Analysis

8.8 Strength of Function

Strength of function rating of SOF-basic was claimed for this TOE to meet the EAL2 assurance requirements. This SOF is sufficient to resist the threats identified in Section 3. Section 4 provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Section 8 demonstrates that the security objectives for the TOE and the TOE environment are satisfied by the security requirements. The evaluated TOE is intended to operate in commercial and DoD low robustness environments processing unclassified information.

The overall TOE SOF claim is SOF-basic because this SOF is sufficient to resist the threats identified in Section 3 Section 8.1 provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Section 8.2 demonstrates that the security objectives for the TOE and the TOE environment are satisfied by the security requirements.

The relevant security functions and security functional requirement that has probabilistic or permutational functions is FIA_UAU.2

9 Acronyms and Terminology

9.1 Acronyms

Table 14 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CC	Common Criteria
CGI	Common Gateway Interface
CLI	Command Line Interface
EAL	Evaluation Assurance Level
EMS	Enterprise Management Server
GB	Gigabyte
GUI	Graphical User Interface
IDS	Intrusion Detection System
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
MD5	Message Digest Five
NIDS	Network Intrusion Detection System
NTLM	NT LAN Manager
OS	Operating System
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
SOF	Strength of Function
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User Datagram Protocol

9.2 Terminology

Analyzer data – Data collected by the Analyzer functions.

Analyzer functions – The active part of the Analyzer responsible for performing intrusion analysis of information that may be representative of vulnerabilities in and misuse of IT resources, as well as reporting of conclusions.

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 Administrators – A subset of authorized users that manage an IDS component.

Authorized User - A user that is allowed to perform IDS functions and access data.

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 which 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.

Packet - A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.

Packet Sniffer - A device or program that monitors the data traveling between computers on a network.

Protection Profile (PP) - An implementation-independent set of security requirements for a category of TOEs 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.

System data – Data collected and produced by the System functions.

System functions – Functions performed by all IDS component (i.e., Analyzer functions, Scanner functions, and Sensor functions).

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.

Trojan Horse - An apparently useful and innocent program containing additional hidden code which allows the unauthorized collection, exploitation, falsification, or destruction of data.

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

User – Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Virus - A program that can "infect" other programs by modifying them to include a, possibly evolved, copy of itself.

Vulnerability - Hardware, firmware, or software flow 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 or disrupt critical processing.