Security Target

For

symantec™

MANHUNT

A NETWORK INFRASTRUCTURE SECURITY PRODUCT

FOR

ATTACK DETECTION, ANALYSIS AND RESPONSE, V.2.11

$DATE: 2003/11/06 10:20:25 $

VERSION .05
$REVISION: 1.24 $

PREPARED BY:

Computer Sciences Corporation
132 National Business Parkway
Annapolis Junction, MD 20701
and
Leroy Lacy, Armadillo Systems, Inc.

For

symantec™

Symantec
Pacific Shores Center
1600 Seaport Blvd., Suite 400
Redwood City, CA 94063

Date	Version	Changes Made
September 13, 2002	0.01	Original Draft
April 10, 2003	0.02	PP compliance dropped
April 17, 2003	0.03	Corrected problems identified
June 12, 2003	0.04	Clarified and modified environmental factors
July 11, 2003	0.05	Clarified assumptions added FIA_UAU.2

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

1 This Section presents security target (ST) identification information and an overview of the ST. An ST document provides the basis for the evaluation of an information technology (IT) product or system (e.g., Target of Evaluation). An ST principally defines:

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

1.1 Identification

2 Title: Security Target for ManHunt: A Network Infrastructure Security product for Attack Detection, Analysis and Response, V.2.11

3 Version: v.05

4 Publication Date: July 11, 2003

5 Authors: Computer Sciences Corporation, Leroy Lacy, Armadillo Systems, Inc

6 Evaluation Assurance Level (EAL) – EAL 3

7 Common Criteria Identification – Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999

8 International Standard – ISO/IEC 15408:1999

9 Keywords: intrusion detection, intrusion detection system, sensor, analyzer

1.2 Overview

10 Symantec Corporation's ManHunt product is an intrusion detection system (IDS) dedicated to reducing network security risk from network intrusion and Denial of Service (DoS) attacks. ManHunt is a software product deployed on dedicated hardware that resides in the same location as the switches and other network devices that are carrying

the traffic to be monitored. The main components of the ManHunt software are the Sensors, Correlation Analysis Framework, Knowledge Base, and Administration Console, or simply console. All of the components, with the exception of the Administration Console, reside on the ManHunt host. The Console, which is used to configure and monitor ManHunt, can be optionally located remotely on any Java-enabled system with network access to the ManHunt hosts.

1.2.1 ManHunt Security Functionality

11 The ManHunt software provides the following intrusion detection system (IDS) security functionality:

- Detection through monitoring of IT resources within the administrative domain and the collection of data/evidence about network traffic events (IDS_SDC),
- Detection through analysis of collected data and response (IDS_ANL),

12 In addition to the IDS security functionality, ManHunt provides the following security functionality to safeguard the integrity of network being monitored.

- Security Management of the IDS security functionality (IDS_FMT), and
- Protection of the IDS security functionality (IDS_FPT).

1.2.2 Intended Environment

13 ManHunt has been designed and developed for commercial and government distributed high-speed switched networks with access to the Internet. It provides roaming sensors, high-speed detection, multi-segment monitoring, and clustered deployment that includes monitoring Network Interface Cards (NICs), switches, routers, and gateways.

1.2.3 Protected Assets

14 Organizations with Internet connectivity are at risk for having their Web sites hacked and their customer data compromised through network intrusion and denial of service (DoS) attacks. The objective of ManHunt is to discover the attacks as they happen and actively protect network resources.

1.3 Conformance Claims

15 This ST makes the following conformance claims:

a) Part 2 Extended: Common Criteria Identification – Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999, (ASE_SRE criteria applicable to this ST).

b) Part 3 Conformant: Common Criteria Identification – Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999, EAL3 level of assurance

16 This ST does not claim Protection Profile conformance.

1.4 Conventions

17 The requirements in this document are divided into assurance requirements and two sets of functional requirements. The first set of functional requirements, which were drawn from the Common Criteria, is designed to address the core System requirements for self-protection. The second set of requirements, which were created and categorized by the short name, IDS, is designed to address the requirements for the System's primary function, which is IDS collection of data and responses to conclusions based upon that data.

18 The CC permits four functional component operations — assignment, refinement, selection and iteration — to be performed on functional requirements. This ST will highlight the four operations in the following manner:

The *assignment* operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets [assignment_value(s)] indicates an assignment.

The *refinement* operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.

The *selection* operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text.*and

Iterated functional components are given unique identifiers by appending to the component name, short name, and functional element name from the CC an iteration number inside parenthesis, i.e., FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2).

Plain *italicized text* is used to emphasize text.

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

1.5 Terms

20 The following table contains terminology specific to the ManHunt TOE that is used throughout the ManHunt ST.

Table 1. ManHunt Terminology

ManHunt Term	Description
Administrative Domain	The logical collection of network devices monitored by a single ManHunt or ManHunt cluster.
Administrative Network	A separate physical network attaching ManHunt nodes to the ManHunt console.
Authorized Administrator	A human user assigned the role of Console Administrator.

Base events	A *base event* is a single instance of an event type. The following is an example of four base events that make up an event type named *Fragmentation Attack event type.*
	`RCRS/IP_FRAG_ODDLENGTH`
	`RCRS/IP_FRAG_OVERDROP`
	`RCRS/IP_FRAG_TEARDROP`
	`RCRS/IP_FRAG_NOMATCH`

Event Types	Event types are group names for one or more *base events*.
Ethernet copy ports	Ethernet copy ports refer to NIC interfaces on the ManHunt or network devices capable of up to 100Mb, one-way, of Ethernet traffic.
Inadvertent Activity	Activity on the monitored network(s) that is not of malicious intent.
iButton	Cryptographic hardware token attaching to a computer serial port via a connector. Product of Dallas Semiconductor Company (www.ibutton.com/java.html).
Incidents	An *incident* is a possible attack and is made up of multiple related *event types*. When the sensor detects a suspicious event, it correlates the event to the incident containing related events. Incidents derive their names from the highest priority event type correlated to the incident.

ManHunt Term	Description
ManHunt cluster	Within a network, multiple ManHunt nodes can work together as a ManHunt cluster and share event data. A ManHunt cluster can comprise up to 100 ManHunt nodes across multiple network segments within multiple network locations.
ManHunt Primary master node secondary master and slave node	By default, the first ManHunt installation is designated to be a primary master node, and all other ManHunt nodes within the cluster are designated to be slave nodes. Changes made on a master node will be propagated to the slave nodes in a cluster.
ManHunt Secondary master node	A secondary master node may be added to help distribute the database synchronization load, or to serve as a backup if the primary master node fails for any reason.
ManHunt Slave node	Slave nodes receive updates to their topology, policy and configuration databases from a master ManHunt node in the cluster.
MSA	ManHunt Smart Agent - A Symantic developed module that enables ManHunt to accept event data from external sensors.
Console Administrator	ManHunt restricts the ability to make changes to the system data and audit data to the *console administrator* through the console. *Console Administrators* have root on UNIX systems and System Administration rights on Windows.
SMON	Switch Monitoring
SPAN	Switch Port Analyzer
Users	*Users* may add comments to incidents, but have no other access to modify system or audit data.

1.6 Document Description

21 In addition to this Introduction section, this ManHunt ST contains the following sections:

Section 2: TOE Description – This section defines the ManHunt IDS components and security functionality initially identified in the overview presented in this section. Section 2 also establishes the logical and physical boundaries for the evaluation of the ManHunt Target of Evaluation (TOE).

Section 3: TOE IT Environment – This section defines the TOE IT environment by identifying all assumptions about the intended environment. The environment is further defined by identifying all threats to the TOE and to the physical environment in which the TOE is located. In addition to the assumption and threat identification, this section identifies and describes all the organizational security policies the operational TOE must implement.

Section 4: Security Objectives – This section identifies the security objectives for the ManHunt TOE and its supporting environment based on the assumptions, threats, and OSPs identified in *Section 3 TOE IT Environment*.

Section 5: IT Security Requirements – This section defines the security functional requirements (SFRs) for the ManHunt TOE. Additionally, explicitly stated requirements (SREs) for the IDS security functionality are also defined. This section also identifies the EAL3 assurance requirements as stated Part 3 of the CC.

Section 6: TOE Summary Specification – This section details how the ManHunt TOE implements each SFR and SRE defined in Section 5.

Section 7: PP Compliance – This ST does not claim compliance with any protection profile.

Section 8: Rationale – This section provides a demonstration of how the information in the ManHunt ST is presented in a consistent, coherent, and comprehensive manner that satisfies all the evaluation requirements for a ST as defined in the Common Criteria Evaluation Methodology (CEM). The demonstration is performed through mapping of assumptions, threats, and OSPs to security objectives. Security objectives are mapped to SFRs and SREs that satisfy the objectives or aspects of the objectives. Rationales and justifications are provided as to why the mappings are appropriate. Also provided are justifications for the chosen assurance levels and strength-of-function (SOF). The information provided in Section 8 collectively represents that the set of security requirements in Section 5 forms a mutually supportive whole.

2 TOE DESCRIPTION

2.1 Product Type

22 ManHunt is a network infrastructure security software product residing on a Solaris 8 platform deployed on dedicated hardware that resides in the same location as the switches and other network devices that are carrying the traffic to be monitored. ManHunt protects the network and systems under its surveillance by monitoring traffic that pass over the network components with ManHunt sensors looking for nonstandard traffic and then analyzes the anomalies to determine if they present a threat to the components in the network. Should the traffic be determined as potentially threatening, the ManHunt analyzer sends alerts to the ManHunt console or performs predetermined actions (e.g., SNMP alert, Allow Handoff, Trackback).

23 Sensors allow ManHunt to effectively monitor many ports. The sensors use switch port analyzers (SPAN) to listen to network flows that are directly attached to the sensors by copying all of a particular port's incoming or outgoing traffic to another port. This enables sensors to monitor 100% of the traffic on the ports they are monitoring without slowing down the traffic. The Switch/Router Communication Module sets copy ports on switches so that the sensors can listen to traffic on the appropriate interfaces. When a sensor detects an attack the information is passed on to FlowChaser.

24 FlowChaser receives network flow data from Cisco routers and ManHunt sensors, and stores the data in an optimized fashion to accelerate the TrackBack process and provide flow information on attacker and victim hosts. FlowChaser also receives data from the Availability Monitor, which monitors user configured hosts on the network and generates an event when any monitored hosts become unresponsive. FlowChaser collects data on current network connections as reported by ManHunt sensors or configured Cisco routers. Flow-Chaser will also recommend QoS (Quality of Service) measures to take if availability of network resources suddenly falls, so that historical traffic flow is preferred over the change. That is, it will suggest access lists that will allow you to discriminate in favor of "normal" traffic over attack traffic.

25 The ManHunt Smart Agent (MSA) enables ManHunt to accept event data in real time from external sensors, such as ManTrap, as well as from third-party sensors. The MSA event coordinator receives the event data and sends it to the analysis framework for aggregation and correlation with all other ManHunt events. ManHunt MSAs are considered remote trusted IT products.

26 ManHunt can hand off and receive data about attacks to/from other ManHunt administrative domains to provide trackback information on the source of an attack.

27 The ManHunt analysis framework aggregates event data on possible attacks from all event sources. The analysis framework also performs statistical correlation analysis on

events to identify event patterns that vary significantly from usual network activity and to identify individual events that are highly related, such as a port scan followed closely by an intrusion attempt.

28 ManHunt uses several databases from which it gathers information about attacks, the network topology, and ManHunt policies, and uses this information, along with data from the sensors, to determine which action(s) to take in response to the attack. For example, it might begin tracking the attack back to its source or hand off the event to another ManHunt. If a policy is set to send an email or SNMP alert, the alerting module does so. The FlowChaser database can be used to quickly determine where an attack is entering the network, and if you supply ManHunt with the appropriate router passwords, the Switch/Router Communication Module can place Access Control Lists (ACLs) on appropriate routers to track flows back to their source.

29 The QSP proxy is a proprietary protocol that enables secure, encrypted communication between the master node and the administration console, and between ManHunt nodes within the same cluster. From the administration console, the ManHunt system administrator can perform tasks, such as configuring the system, editing the topology and policy databases, monitoring attack incidents in progress, and generating reports. Changes to the configuration, topology or policy databases can be made to a master ManHunt node that will subsequently push the updates to the other ManHunt nodes in the cluster.

30 The reporting module can automatically generate and send daily email reports on the most frequently occurring event types for the day. For a greater level of detail, the reporting module can also generate graphical reports on demand from the administration console. These reports provide detailed data on the types of events and incidents that occurred and protocols exploited during the specified time period.

31 Within a network, multiple ManHunt nodes can work together as a ManHunt cluster and share event data. A ManHunt cluster can comprise up to 100 ManHunt nodes across multiple network segments within multiple network locations. Each cluster will have a master node (and possibly a backup master node) and slave nodes.

2.2 Physical Scope and Boundary

32 The following figure graphically illustrates the TOE Physical Boundary. The figure represents one ManHunt Cluster including an administrative network.

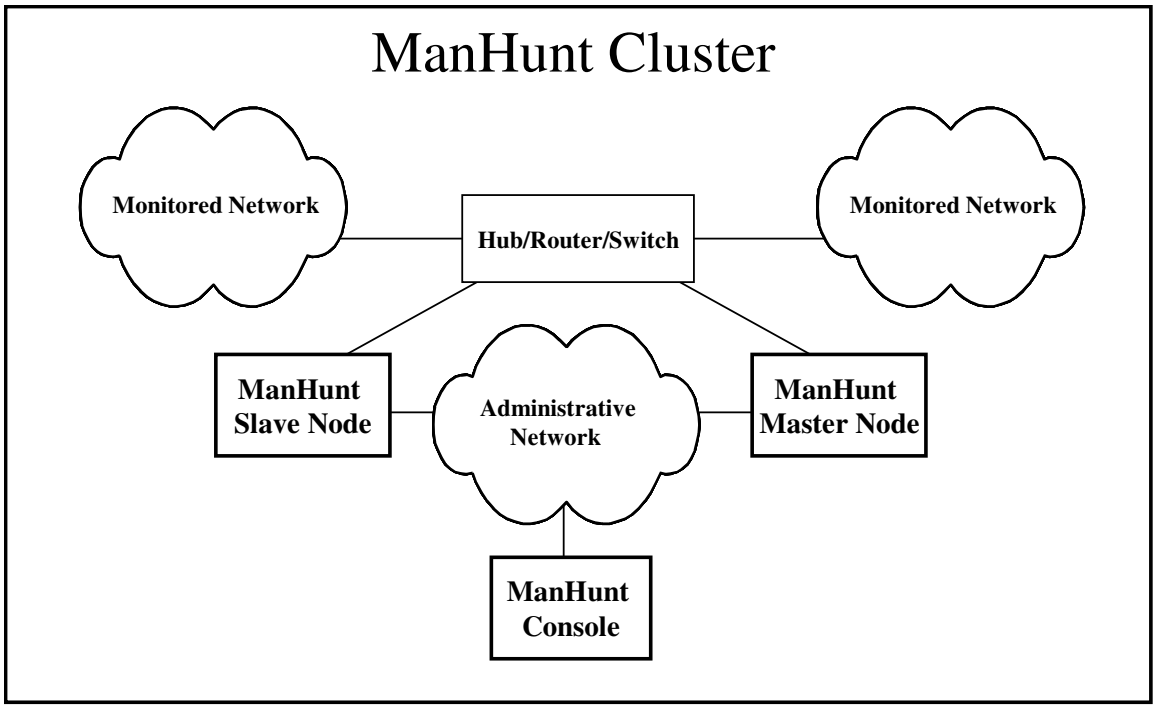

Figure 1 Physical TOE Boundary

2.2.1 Evaluated Configuration

33 The following table summarizes the categories of configuration items of the evaluated TOE and identifies all the IDS components included in the evaluated configuration. The subset of configuration items detailed in the Table represents the evaluated TOE.

Table 2. TOE Configuration Items

CI Categories	ManHunt Components
ManHunt Version 2.11 Software (1 or more instances of ManHunt Software to form ManHunt Nodes within Cluster)	**Administration Console** (1 for Cluster)
	ManHunt (2.11) Host/Node

2.2.2 Evaluated TOE Configuration

34 The evaluated TOE consists of the ManHunt Version 2.11 Software configured on the Solaris 8 platform residing on the following dedicated hardware as part of a distributed high-speed switched network with access to the Internet. The ManHunt Administration Console can operate on Solaris 8 or Microsoft Windows 95/98/NT/2000 platform.

Table 3. Evaluated TOE System Requirements

	System Requirements
ManHunt Node	SPARC platform
	1 Gigabyte RAM
	Sun Solaris 8

	Multiple CPUs supported (1-4)
	1 network interface for general communication and administration
	1 network interface for each monitored device
ManHunt Node	Intel P3
	Sun Solaris 8
	1 network interface for general communication and administration
	1 network interface for each monitored device
Administration Console	SPARC platform
	Java 2 Runtime Environment v 1.3
	Solaris 2.6/7/8
Network Devices	Dynamic port configuration requires SMON capable switches
	Static port monitoring may be performed on any switch or hub

2.2.3 Excluded from the TOE Evaluation

The items listed below are specifically excluded from the evaluation of the TOE.

- Solaris OS
- Handoff Coordinator
- Open SSH

2.3 Logical Scope and Boundary

35 The TOE logical boundary consist of the following security functions controlled by ManHunt:

- Detection through monitoring of IT resources within the administrative domain and the collection of data/evidence about network traffic events, (IDS_SDC)
- Detection through analysis of collected data and response, (IDS_ANL)
- Security Management of the IDS security functionality, (IDS_FMT) and
- Protection of the IDS security functionality. (IDS_FPT)

2.3.1 ManHunt Security Functions

2.3.1.1 IDS_SDC Detection Through Monitoring of IT Resources

36 Sensors take information from each of the monitored switches and classify events as either legitimate or "suspicious (anomalous)". Suspicious (anomalous) events are passed up to the Analysis Framework, where related events are grouped as incidents and evaluated "in context" to determine their severity.

37 FlowChaser receives network flow data from Cisco routers and ManHunt sensors, and stores the data in an optimized fashion to accelerate the TrackBack process and provide flow information on attacker and victim hosts. FlowChaser also receives data from the Availability Monitor, which monitors user configured hosts on the network and generates an event when any monitored hosts become unresponsive. FlowChaser collects data on current network connections as reported by ManHunt sensors or configured Cisco routers. Flow-Chaser will also recommend QoS (Quality of Service) measures to take if availability of network resources suddenly falls, so that historical traffic flow is preferred over the change. That is, it will suggest access lists that will allow you to discriminate in favor of "normal" traffic over attack traffic.

38 The ManHunt Smart Agent (MSA) enables ManHunt to accept event data in real time from external sensors, such as ManTrap, as well as from third-party sensors. The MSA event coordinator receives the event data and sends it to the analysis framework for aggregation and correlation with all other ManHunt events. ManHunt MSAs are considered remote trusted IT products.

2.3.1.2 IDS_ANL Detection through analysis of collected data and response

39 ManHunt is designed with an analysis layer, Analysis Framework, operating above the sensors, which adds additional information to the raw sensor data and presents a more complete picture of security-related activities on the network.

40 ManHunt responds to intrusion detection in a number of ways from simple notification of the administrator to providing automated responses to protect systems. ManHunt classifies IDS attacks into two categories: Intrusion Attempts and Denial of Service (DoS) Attacks. An intrusion attempt is a much simpler attack to deal with because once it has been identified the connection can be terminated. A DoS attack does not require a connection to be made and the attack consists of very large volumes of data. ManHunt has a variety of administrator configurable automated responses and multiple responses may be configured for one incident.

41 ManHunt uses a separate interface for notification that can be located on an administrative network to increase the likelihood the notification can be sent successfully by lessening the chance of deliberate compromise. While session termination is a response option for ManHunt to stop an attack, nothing is learned of the attacker. When possible, ManHunt employs other response options. ManHunt's Trackback function is designed to automatically track a data stream to the entry point into the administered network.

The TrackBack function is designed to automatically track a data stream to its source within the cluster, or, if the source is outside the cluster, to its entry point into the cluster. The Trackback process can continue beyond the administrative domain through communication with an upstream peer network. ManHunt is designed to both send and receive tracking information across administrative boundaries if policies have been configured to do so. ManHunt hosts may register with each other when communication

between them is desired and ManHunt will only respond to a message from a registered and authenticated ManHunt.

2.3.1.3 IDS_FMT Security Management of the IDS Functionality

42 ManHunt recognizes two types of administrative roles: *Console Administrator* (available from Administration Console) and *User* (also available from Administration Console). The *Console Administrator* can make changes to the topology tree, response policies, and configuration parameters, mark incidents and add incident annotations from the administrative console. The *User*'s privileges are limited to viewing incident data, marking incidents and adding incident annotations.

2.3.1.4 IDS_FPT Protection of Security Functionality

43 ManHunt uses QSP proxy, a proprietary protocol that enables secure, encrypted communication between the ManHunt master node and the Administration Console, and between ManHunt nodes within the same cluster.

44 From the Administration Console, the ManHunt *Console Administrator* can perform tasks, such as configuring the system, editing the topology and policy databases, monitoring attack incidents in progress, and generating reports.

45 Changes to the configuration, topology or policy databases can be made to the ManHunt master node, which will subsequently push the updates to the other ManHunt nodes in the cluster

3 TOE SECURITY ENVIRONMENT

3.1 Secure Usage Assumptions

46 This section describes the security aspects of the intended environment for the evaluated TOE. This includes information about the physical, personnel, procedural, connectivity, and functional aspects of the environment.

47 The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and administrator guidance. The following specific conditions are assumed to exist in an environment where this TOE is employed.

3.2 Assumptions

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

Name	Description	Functional Aspect
A.AUTHORIZED	Only authorized TOE *Users* and *Console Administrators* will have accounts on those platforms on which the TOE executes.	Administrative
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.	Physical
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. (The processing resources of the TOE include the Sensors and monitored IT product, the MSA and monitored IT product, the ManHunt Node(s), and ManHunt Console)	Physical
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.	Personnel
A.PFORM_SPT	The TOE environment must provide reliable platform functions including: correct hardware operation and functionality including providing system time; correct platform software operation and functionality.	Physical
A.ACC_CONTR	The operating systems upon which the Console and Node runs will be configured to restrict modification to TOE executables and configuration files to only the *Console Administrator*.	Functional

Name	Description	Functional Aspect
A.NOEVIL	Authorized *User*s and *Console Administrators* are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.	Personnel

3.3 Threats

49 The following are threats identified, if any, for the TOE and the IT Systems the TOE monitors. The assumed level of expertise of the attacker for all the threats is unsophisticated.

3.3.1 TOE Threats

There are no threats directed at the TOE that the TOE counters. It provides security to the monitored network by identifying and reporting activity that may be malicious in nature.

3.3.2 IT System Threats

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

TE.MISUSE	Unauthorized network accesses and activity indicative of misuse such as introductions of Trojan horses and viruses may occur on an IT System connected to the network the TOE monitors.

3.4 Organizational Security Policies

51 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.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and response actions taken as prescribed by local site policy.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
P.ADMIN	Management functions of the TOE shall be restricted to the Authorized Administrator(s).
P.ACCACT	Human users of the TOE shall be accountable for their actions.
P.MONITOR	The network will be monitored and reports on network activities will be made in accordance with local site policy.

4 SECURITY OBJECTIVES

52 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

53 The following are the TOE security objectives:

O.IDSENS	The TOE must collect and store information about network events that are indicative of inappropriate activity that may have resulted from actual or potential misuse, access, or malicious activity directed against IT System assets attached to the network monitored by the TOE.
O.IDANLZ	The TOE must accept data from ManHunt sensors and remote trusted IT products (Symantic MSAs) and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.RESPON	The TOE must respond to analytical conclusions using TOE policy without human intervention.
O.EXPORT	When a TOE component makes its data available to another TOE component, the TOE will ensure the confidentiality of the data.
O.ADMIN	The TOE must include a set of functions that allow management of its functions and data.
O.SEP_ROLE	The TOE must accommodate separate roles for Authorized Administrators to limit their access to the TOE security mechanisms

4.2 Security Objectives for the Environment

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

OE.DAC	The TOE environment must provide discretionary access control (DAC) to protect TOE executables, TOE data, and host generated audit data.
OE.AUDITS	The host platform must record audit records for data accesses and use of the host system functions.
OE.PLATFORM_ SUPPORT	The TOE environment must provide reliable platform functions including: correct hardware operation and functionality including providing system time; correct platform software operation and functionality.
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.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.

5 IT SECURITY REQUIREMENTS

55 IT security requirements include:

- TOE security requirements, and (optionally)
- TOE's IT Environment security requirements upon which satisfaction of the TOE's security objectives depend.

56 These requirements are discussed separately below.

5.1 TOE Security Requirements

57 The CC divides security requirements into two categories:

- *Security functional requirements (SFRs)*: that is, requirements for security functions such as information flow control, audit, and identification.
- *Security assurance requirements (SARs)*: provide grounds for confidence that the TOE meets its security objectives (for example, configuration management, testing, and vulnerability assessment).

58 These requirements are discussed separately within the following subsections.

5.1.1 TOE Security Functional Requirements

59 Table 4 identifies the Security Functional Requirements (SFRs) for the TOE.

Table 4 TOE Functional Components

Functional Component ID	Functional Component Name	Dependencies
Security Management		
FIA_UAU.2	User Authentication before any action	FIA_UID.1
FMT_MOF.1	Management of security functions behaviour	FMT_SMR.1 FMT_SMF.1
FMT_MTD.1	Management of TSF data	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	Specification of Management Functions	None
FMT_SMR.1	Security roles	FIA_UID.1
Data Protection		
FPT_ITC.1	Inter-TSF confidentiality during transmission	NONE
FPT_ITT.1	Basic internal TSF data transfer protection	NONE
Intrusion Data Collection		
IDS_SDC.1	System Data Collection	NONE
Intrusion Data Analyze		

IDS_ANL.1	Analyzer analysis	NONE
IDS_RCT.1	Analyzer react	NONE

5.1.1.1 Security Management (FMT)

60 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 action on behalf of that user.

61 FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to *modify the behaviour of* the functions [monitored IT system data collection, data analysis and reaction] to [*Console Administrator(s)*].

62 **FMT_MTD.1 (1) Management of TSF data**

FMT_MTD.1.1 The TSF shall restrict the ability to *modify,* [add] the [System and audit data] to [the *Console Administrator*].

63 **FMT_MTD.1 (2) Management of TSF data**

FMT_MTD.1.1 The TSF shall restrict the ability to *modify* **the** [Violations of protocol specifications for monitored network protocols, intrusion related patterns in monitored protocol data streams, network authentication failures, network flood conditions, system information gathering (scanning) attempts; and

a) All packet information from level 3 to level 7 of the TCP/IP protocol and the application data. (EXP)

b) Date and time of the event, type of event, subject identity, and the outcome (e.g. success or failure) of the event; and

c) The additional information specified in the Details column of Table 5.]

to [the *Console Administrator*].

64 **FMT_SMF.1 Specification of Management Functions**

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [data collection,

a) Data analysis, and

b) reaction].

65 **FMT_SMR.1 Security roles**

FMT_SMR.1.1 The TSF shall maintain the roles*:* [*Console Administrator*, and Users].

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

5.1.1.2 Protection of the TOE Security Functions (FPT)

66 **FPT_ITC.1 Inter-TSF confidentiality during transmission**

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

67 **FPT_ITT.1 Basic internal TSF data transfer protection**

FPT_ITT.1.1 The TSF shall protect TSF data transmitted from *disclosure* when it is transmitted between separate parts of the TOE.

5.1.1.3 IDS Explicitly Stated Component Requirements (IDS)

68 **IDS_SDC.1 System Data Collection (EXP)**

IDS_SDC.1.1 The System shall be able to collect the following information from the monitored IT Systems:

a) Violations of protocol specifications for monitored network protocols, intrusion related patterns in monitored protocol data streams, network authentication failures, network flood conditions, system information gathering (scanning) attempts; and

b) All packet information from level 3 to level 7 of the TCP/IP protocol and the application data. (EXP)

IDS_SDC.1.2 At a minimum, the TOE shall collect and record the following information:

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

b) The additional information specified in the Details column of Table 5. (EXP)

Table 5 System Events

Component	Event	Details
IDS_SDC.1	Violation of protocol specifications for monitored network protocols, Intrusion related patterns in monitored protocol data streams, Identification and authentication events	Violation type, protocol type, IP header, IP source address and source port, IP destination address and destination port, location detected, {optionally} full packet that tripped the alarm. User identity, location, source address, destination address.
IDS_SDC.1	Network Authentication failures, Data Access	Violation type, protocol type, IP header, IP source address and source port, IP destination address and destination port, location detected, [optionally] full packet that tripped the alarm. Requested access, source address, destination address
IDS_SDC.1	Network flood conditions, services requests	Violation type, protocol type, IP header of representative packet, IP source address and source port, IP destination address and destination port, location detected, [optionally] full representative packet.
IDS_SDC.1	System information gathering (scanning) attempts	Violation type, protocol type, IP header of representative packet, IP source address and source port, IP destination address and destination port, location detected, [optionally] full representative packet.

69 **IDS_ANL.1 Analyser analysis (EXP)**

IDS_ANL.1.1 The System shall perform the following analysis function(s) on IDS data received:

a) statistical, signature, integrity;
b) Protocol Anomaly Detection,
c) Packet reconstruction from layer 3 to layer 7,
d) Weighted Fair Queuing, event aggregation, and
e) correlation analysis. (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) response. (EXP) IDS_ANL.1.2

70 **IDS_RCT.1 Analyzer react (EXP)**

IDS_RCT.1.1 The System shall send an alarm-to-alarm destination as defined by the Console Administrator configured alerting parameters and take appropriate actions as defined by the Console Administrator configured response policy parameters when an intrusion is detected. (EXP)

5.1.2 Security Requirements for the IT Environment

71 There are no security functional requirements for the IT Environment.

5.2 Assurance Requirements

72 This subsection defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL3 with no augmentation. Table 6 Assurance Components identifies the EAL 3 assurance components satisfied by the TOE.

Table 6 Assurance Components

Assurance Class	Assurance components
Configuration management ACM:	ACM_CAP.3 Authorization controls ACM_SCP.1 TOE CM coverage
Delivery and operation ADO	ADO_DEL.1 Delivery procedures ADO_IGS.1 Installation, generation, and start-up procedures
Development ADV	ADV_FSP.1 Informal functional specification ADV_HLD.2 Security enforcing high-level design ADV_RCR.1 Informal correspondence demonstration
Guidance documents AGD	AGD_ADM.1 Administrator guidance AGD_USR.1 User guidance
Life cycle support ALC	ALC_DVS.1 Identification of security measures
Tests ATE	ATE_COV.2 Analysis of coverage ATE_DPT.1 Testing: high-level design ATE_FUN.1 Functional testing ATE_IND.2 Independent testing – sample
Vulnerability assessment AVA	AVA_MSU.1 Examination of guidance AVA_SOF.1 Strength of TOE security function evaluation AVA_VLA.1 Developer vulnerability analysis

5.3 Security Requirements for the IT Environment

73 There are no security functional requirements for the IT Environment.

5.4 SFRs With SOF Declarations

The overall Strength of Function (SOF) claim for the TOE is SOF-basic.
FIA_UAU.2: The authentication mechanism has a PIN space of 96^6.

6 TOE SUMMARY SPECIFICATION

74 This subsection details the IDS security functionality provided by the ManHunt TOE. The following table traces each IT Security Function to TOE security functional requirements.

Table 7. Tracing TSF to SFRs

IT Security Function	TOE SFR	
IDS_FMT	FIA_UAU.2	User authentication before any action
IDS_FMT	FMT_MOF.1	Management of security functions behaviour
IDS_FMT	FMT_MTD.1 (1)(2)	Management of TSF data
IDS_FMT	FMT_SMR.1 FMT_SMF.1	Security roles
IDS_FPT	FPT_ITC.1	Inter-TSF confidentiality during transmission
IDS_FPT	FPT_ITT.1	Basic internal TSF data transfer protection
IDS_SDC	IDS_SDC.1	System Data Collection
IDS_ANL	IDS_ANL.1	Analyzer analysis System Data Collection
IDS_RCT	IDS_RCT.1	Analyzer react

6.1 Security Management – IDS_FMT

6.1.1 FIA_UAU.2, FMT_MOF.1, FMT_MTD.1, FMT_SMF.1 and FMT_SMR.1

75 FIA_UAU.2, FMT_MOF.1, FMT_MTD.1 (1)(2), and FMT_SMR.1 are satisfied through the following IDS components and functional design:

76 ManHunt recognizes two types of administrative roles: *Console Administrator* and *User*. The *Console Administrator* can make changes to the topology tree, response policies, and configuration parameters, mark incidents and add incident annotations. *User* privileges are limited to viewing incident data, marking incidents and adding incident annotations. Prior to performing any TSF both *Console Administrators* and *Users* must be authenticated. UAU.2 is a permutational mechanism for the authentication of the *Console Administrator* and *User*.

6.2 Protection of the Security Functions – IDS_FPT

6.2.1 FPT_ITC.1 Inter-TSF confidentiality during transmission

77 ManHunt to receives information from other security IT products and displays the information as incident and event data in the ManHunt data store. A Symantec developed module (MSA) is required that interfaces to the security IT product and

collects certain information and then communicates securely with ManHunt to present the information to the analysis framework. For the purposes of this evaluation, the MSAs are considered a remote trusted IT product.

6.2.2 FPT_ITT.1 Basic internal TSF data transfer protection

78 All ManHunt nodes within an administrative domain will automatically communicate with each other and share information and resources as necessary to gather additional information about an attack or track it back across the network to locate the entry point of an attack into the protected network. This trusted communication takes place through a protocol service that uses triple-DES encryption and a configurable port number.

6.3 Detection through monitoring of IT resources within the administrative domain and the collection of data/evidence about network traffic events (IDS_SDC)

6.3.1 IDS_SDC.1 System Data Collection:

79 Symantec ManHunt satisfies the IDS_SDC.1 through the following IDS components and functional design:

80 With steerable sensors, ManHunt gathers its primary detection data directly from switches through copy ports. If the switch is SMON capable, ManHunt can dynamically reassign the ports that are copied to the sensors, giving the ability to monitor all ports over a period of time. This dynamic reassignment is called “roaming”. Roaming capability permits ManHunt to monitor 100 percent of traffic on a port for a period of time to ascertain the full state of all communications on that port. If there is nothing of interest taking place on that port, ManHunt can select another port to monitor.

6.4 Detection through analysis of collected data and response (IDS_ANL)

6.4.1 IDS_ANL.1 Analyzer analysis

81 Symantec ManHunt satisfies the IDS_ANL.1 through the following IDS components and functional design:

82 ManHunt is designed with an analysis layer, Analysis Framework, operating above the sensors, which adds intelligence to the raw sensor data and presents a more complete picture of security-related activities on the network. One benefit of this approach is that it provides the ability to create phased responses and minimize false positives. Also, the analysis after the detection by the sensors helps to make sense of the events taking place on the network and to evaluate them in context.

83 ManHunt’s Protocol Anomaly Detection technology analyzes network traffic using a combination of techniques that relies primarily on its ability to recognize activity that is

unusual, unexpected, or in violation of legitimate communication behavior. ManHunt sensors model appropriate communication and consider deviation from that model to be suspicious. ManHunt uses protocol and state machine models that are custom designed to perform in a security role in that there is acknowledgement that legitimate business communications often deviate slightly from the strict protocol models. Protocol Anomaly Detection also recognizes that legal and legitimate traffic can actually be an attack.

84 By understanding how legitimate communications typically take place over all major protocols, ManHunt sensors identify not only known attacks, but also most new and novel attacks that could be missed by signature-based methods. ManHunt does use the signature approach for a small set of attacks where the anomaly method is not as sensible as the signature method.

85 ManHunt sensors incorporate a statistical, or rate counter component to identify DoS or flood attacks. This element is self-tuning, recognizing that different environments and organizations can experience vastly different types of traffic.

86 ManHunt sensors operate on de-fragmented packets and perform reconstruction from layer 3 to 7 of the OSI model.

87 Built into ManHunt's multiple layer analysis architecture is a security mechanism called Weighted Fair Queuing that provides a filter for data entering the Analysis Framework from the sensors. This filtering process helps process potentially huge amounts of data while insuring the integrity of the system by protecting it from flood attacks and standard IDS evasion techniques.

88 **Weighted Fair Queuing:** Packets are distributed over a set of queues based upon similar packet characteristics, and each queue is serviced equally. The sorting algorithm is designed to maximize the likelihood that packets from the same attack will be assigned to the same queue and that different attacks will be assigned to different queues. If the rate of incoming packets exceeds ManHunt's ability to process them, the packets that get discarded are the oldest ones in the queue to which the new packets would be assigned.

89 Packets are analyzed in the order in which they reach the heads of their respective queues, rather than the order in which they arrive. This reduces the risk of a packet flood obscuring the real attack.

90 **Event Aggregation:** In order to evaluate an event "in context", the Analysis Framework groups related events into Incidents. Events are judged related if they share some common characteristics such as type, source or destination. When an event percolates up from the sensors, the Analysis Framework considers its characteristics to decide whether it is part of an existing incident. If it is, it gets added to that incident; otherwise a new incident is created. If no new events are added to an incident for a predetermined period

of time, the incident expires. Subsequent events that might otherwise have been associated with an expired incident will be aggregated in a separate incident. The expiration time for an incident is administrator configurable quantity.

91 **Correlation Analysis:** Correlation Analysis is about integrating multiple and disparate raw data sources with a knowledge base that can help to make sense of it. It brings all of the data together in a single user interface for management, configuration, and monitoring. One ManHunt host in the process of evaluating a potential threat in one part of the network can directly control sensor resources and share knowledge base information from another ManHunt. Statistical data is also collected and shared to expand the scope of threats that can be addressed.

6.4.2 IDS_RCT.1 Analyzer react

92 Symantec ManHunt satisfies the IDS_RCT.1 through the following IDS components and functional design:

93 ManHunt responds to intrusion detection in a number of ways from simple notification of the administrator to providing automated responses to protect systems. ManHunt classifies IDS attacks into two categories: Intrusion Attempts and Denial of Service (DoS) Attacks. An intrusion attempt is a much simpler attack to deal with because once it has been identified the connection can be terminated. A DoS attack does not require a connection to be made and the attack consists of very large volumes of data. The following subsections describe ManHunt's automated responses and how the rules for applying them are contained in the policy configuration of ManHunt. Multiple responses may be configured for one incident.

94 **Notification:** ManHunt uses a separate interface for notification that can be located on an administrative domain to increase the likelihood the notification can be sent successfully by lessening the chance of deliberate compromise. Notification is of 5 types: administration console visual, administration console auditory, email notice of event, SNMP trap for an event, email summary reports. The email summary reports include the report start time, node number of the ManHunt that generated the report, ManHunt login history with the source IP and time of the login event, event types that occurred most frequently during the report period, the number of times each event type occurred, event source IP addresses and number of time address occurred, event destination IP addresses and number of times address occurred, highest severity incidents with source and destination IP addresses, and time incident occurred.

95 **Session Termination:** While session termination is a response option for ManHunt to stop an attack, nothing is learned of the attacker. When possible, ManHunt employs other response options.

96 **Trackback:** ManHunt's Trackback function is designed to automatically track a data stream to the entry point into the administered network. Trackback uses special sensors

designed to search the network systematically looking at the data stream with matching characteristics via communications with switches, routers and other ManHunt hosts within the administrative domain. Using its knowledge of the network topology, ManHunt interrogates devices about the attack stream and prioritizes possible paths. To accomplish this process, one ManHunt node can grab sensor resources from another ManHunt node. The Trackback process can continue beyond the administrative domain through communication with an upstream peer network. The default format for this communication is authenticated e-mail message to the network administrator

97 When interrogating devices in the Trackback process, ManHunt interacts with both switches and routers. Typically, ManHunt is connected directly to switch ports and then can dynamically reconfigure copy ports as necessary if the switch is SMON capable. ManHunt has multiple methods for communicating with routers based on manufacturer and network engineer preferences. Options are RMON for routers supporting this protocol and telnet for routers with ENABLE privileges and setting the router to debug mode.

6.5 TOE Assurance Measures

98 The TOE provides the following EAL 3 assurance measures as evidenced in the following subsections identifying appropriate documentation detailing the measures.

Assurance Component	How requirement will be met
ACM_CAP.3 Authorization controls	The vendor has provided documentation for the configuration management of the ManHunt product.
ACM_SCP.1 TOE CM coverage	The vendor has provided documentation for a configuration management system.
ADO_DEL.1 Delivery procedures	The vendor has provided delivery documentation.
ADO_IGS.1 Installation, generation, and start-up procedures	The vendor has provided Installation Procedures.
ADV_FSP.1 Informal functional specification	The vendor has provided design documentation.
ADV_HLD.2 Security enforcing high-level design	The vendor has provided design documentation.
ADV_RCR.1 Informal Correspondence demonstration	The informal Correspondence Demonstration has been provided as a part of the Design Documentation

AGD_ADM.1 Administrator guidance	The vendor has provided documentation for Administrator Guidance.
AGD_USR.1 User guidance	None – All access to the ManHunt TSF is by privileged users (Administrative)
ALC_DVS.1 Identification of security measures	The vendor has provided evidence of ALC_DVS.1 Compliance and supporting documents.
ATE_COV.2 Analysis of coverage	The vendor has provided documentation for analysis of coverage.
ATE_DPT.1 Testing: high-level design	The vendor has provided documentation for testing of the high level design for the TSF's.
ATE_FUN.1 Functional testing	The vendor has provided documentation of the functional testing of the TOE.
ATE_IND.2 Independent testing – sample	The laboratory used development evidence submitted by the vendor along with the functional testing evidence as a baseline for an independent test plan.
AVA_MSU.1 Examination of guidance	The vendor has provided evidence for ADO_IGS, ADV_FSP, and AGD_ADM, which will be utilized to meet this requirement.
AVA_SOF.1 Strength of TOE security function evaluation	The vendor has provided SOF data for functions where required.
AVA_VLA.1 Developer vulnerability analysis	The vendor has provided vulnerability documentation.

7 PP COMPLIANCE

99 This ST does not claim compliance to any Protection Profile

8 RATIONALE

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

101 This section is a demonstration of how the information in the ManHunt ST is presented in a consistent, coherent, and comprehensive manner that satisfies all the evaluation requirements for a ST as defined in the Common Criteria Evaluation Methodology (CEM). The demonstration is performed through mapping of assumptions, threats, and OSPs to security objectives. Security objectives are mapped to SFRs and SREs that satisfy the objectives or aspects of the objectives. Rationales and justifications are provided as to why the mappings are appropriate. Also provided are justifications for the chosen assurance levels and strength-of-function (SOF). The information provided in Section 8 collectively represents that the set of security requirements in Section 5 forms a mutually supportive whole.

8.1 Rationale for IT Security Objectives

102 This section provides a rationale for the existence of each assumption, threat, and policy statement that compose the ManHunt System Security Target. Table 8 Security Environment vs. Objectives 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 8 Security Environment vs. Objectives

	O.IDSENS	O.IDANLZ	O.RESPON	O.EXPORT	O.ADMIN	O.SEP_ROLE	OE.PFORM_SPUPPORTT	OE.DAC	OE.AUDITS	OE..INSTAL	OE.PHYCAL
A.AUTHORIZED										X	
A.PROTCT										X	
A.LOCATE											X
A.MANAGE										X	
A.PFORM_SPT							X				X
A.ACC_CONTR								X		X	
A.NOEVIL										X	
P.ACCACT								X	X		
P.ADMIN					X	X		X		X	
P.ANALYZ		X	X								
P.INTGTY								X			

	O.IDSENS	O.IDANLZ	O.RESPON	O.EXPORT	O.ADMIN	O.SEP_ROLE	OE.PFORM_SPUPPORTT	OE.DAC	OE.AUDITS	OE..INSTAL	OE.PHYCAL
P.MONITOR	X	X	X	X							
TE.MISUSE									X		

103 A.AUTHORIZED Only TOE *Users* and *Console Administrators* will have accounts on those platforms on which the TOE executes. OE.INSTAL provides for the installation management and operation of the TOE consistent with IT security.

104 A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification. OE.INSTAL provides for the installation management and operation of the TOE consistent with IT security. The OE.PHYCAL provides for the physical protection of the TOE.

105 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.

106 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.INSTAL objective ensures the TOE is managed and operated in a manner, which is consistent with IT security.

107 A.PFORM_SPT The TOE environment must provide reliable platform functions including: correct hardware operation and functionality including providing system time; correct platform software operation and functionality. The OE.PFORM_SUPPORT objective provides for the proper operation of the platform on which the TOE resides. OE.PHYCAL ensures the platform is secure from physical attack.

108 A.ACC_CONTR The operating systems upon which the Console and Node runs will be configured to restrict modification to TOE executables and configuration files to only Authorized *Console Administrator*. OE.DAC provides discretionary access control for the protection of the TOE. The OE.INSTAL objective ensures the TOE is managed and operated in a manner, which is consistent with IT security.

109 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.

110 P.ACCACT Users of the TOE shall be accountable for their actions within the IDS. The OE.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions.

111 P.ADMIN Management functions of the TOE shall be restricted to *Console Administrator*. The O.ADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTAL objective supports the objective by ensuring administrators follow all provided documentation and maintain the security policy. The OE.DAC objective provides for authentication of users prior to any TOE function accesses. The TOE must accommodate separate roles for Authorized Administrators to limit their access to the TOE security mechanisms, O.SEP_ROLE.

112 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 the Sensors. O.RESPON requires the TOE to respond to analytical conclusions based upon TOE policy without human intervention.

113 P.INTGTY Data collected and produced by the TOE shall be protected from modification. The OE.DAC objective restricts access to TOE data stores to ensure the protection of data from modification.

114 P.MONITOR The TOE will monitor the network and report on network activities. The TOE must collect and store information about events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets monitored by the TOE. (O.IDSENS). The TOE must accept data from ManHunt Nodes and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future). (O.IDANLZ). When TOE components make its data available to another TOE component, the TOE will ensure the confidentiality of the data. (O.EXPORT). O.RESPON requires the TOE to respond to analytical conclusions based upon TOE policy without human intervention.

115 TE.MISUSE Unauthorized accesses and activity indicative of misuse such as introductions of Trojan horses and viruses may occur on an IT System the TOE monitors. The OE.AUDITS requires the host record audit records of data accesses and the use of system functions.

8.2 Rationale for Security Objectives for the Environment

116 The purpose for the environmental objectives is to provide protection for the TOE that cannot be addressed through IT measures. The defined objectives provide for physical protection of the TOE, proper management of the TOE, and interoperability requirements on the TOE. Together with the IT security objectives, these environmental objectives provide a complete description of the responsibilities of TOE in meeting security needs.

8.3 Rationale for Security Requirements

117 This section demonstrates that the functional components selected for the ManHunt System ST and provides complete coverage of the defined security objectives. The mapping of components to security objectives is depicted in the following table.

Table 9 Requirements vs. Objectives Mapping

	O.IDSENS	O.IDANLZ	O.RESPON	O.EXPORT	O.ADMIN	O.SEP_ROLE
FIA_UAU.2					X	X
FMT_MOF.1						X
FMT_MTD.1(1)					X	
FMT_MTD.1(1)					X	
FMT_SMF.1						X
FMT_SMR.1						X
FPT_ITC.1				X		
FPT_ITT.1				X		
IDS_SDC.1	X					
IDS_ANL.1		X				
IDS_RCT.1			X			

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

119 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. These events must be defined in the ST [IDS_SDC.1].

120 O.IDANLZ The Analyzer must accept data from IDS Sensors 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].

121 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].

122 O.EXPORT When any IDS component makes its data available to another IDS component, 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_ITC.1, FPT_ITT.1].

123 O.ADMIN The TOE must include a set of functions that allow management of its functions and data. Only authorized administrators of the System may query or add audit and System data [FIA_UAU.2, FMT_MTD.1(1)(2)].

124 O.SEP_ROLE The TOE must accommodate separate roles for Authorized Administrators to limit their access to the TOE security mechanisms. The TOE must be able to maintain separate security roles Console administrator and console user [FIA_UAU.2, FMT_SMR.1, FMT_SMF.1, FMT_MOF.1]

8.4 Rationale for Assurance Requirements

125 EAL3 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 EAL3, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

8.5 Rationale for Explicitly Stated Requirements

126 The family of IDS requirements was derived from the [IDS_SYS_PP] as they 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.

8.6 Rationale for Strength of Function

127 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.

8.7 Rationale for the TOE Summary Specification

128 The information in this subsection is provided to demonstrate that the TOE TSF functionality described in Section 6 of this ST satisfies the SFRs, that the TOE summary specification confirms and supports the tracing of threats/policies to objectives and the tracing of objectives to SFRs that serve to meet those objectives.

8.7.1 Suitability of TOE TSF to satisfy TOE SFRs.

129 Table 7 traces all the SFRs to TOE Security Functions TSF as identified in Section 2, TOE Description of this ST. Sections 6.1 through 6.5 detail how the TOE TSF provide the functionality to satisfy the SFRs identified in Section 5 of this ST.

8.7.2 Strength of Function

130 The overall TOE SOF claim is SOF-basic because this SOF is sufficient to resist the threats identified in Section 3.3. Section 8.1 provides evidence that demonstrates that TOE threats are countered by the TOE security objective. Section 8.2.1 demonstrates that the security objectives for the TOE and the TOE environment are satisfied by the security requirements. The SOF-basic claim for the TOE applies because access to the TOE is protected against an attacker of limited ability with no special tools.

8.7.3 Tracing of Assurance Measures to SARs.

131 Section 6.4 traces each EAL3 security assurance requirement (SAR) identified in Section 5.2 and relates the SAR to the evaluation evidence/document that provides the assurance measures.

8.8 Rationale for Satisfying All Dependencies

132 Below is a cross-reference of the functional components, their related dependencies, and whether the dependency was satisfied. As evidenced by Table 10, all of the dependencies have been satisfied with the exception of FIA_UID.1. FIA_UID.1 states that certain TSF functions can be performed prior to being authenticated, but the TOE requires authentication prior to performing any TSF functions. A passphrase is used upon login to the TOE that identifies the passphrase with a role. Therefore, the satisfaction of FIA_UID.1 is not applicable.

Table 10 Requirement Dependencies

Functional Component	Dependency	Included
FIA_UAU.2	FIA_UID.1	NO
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	YES
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	YES
FMT_SMR.1	FIA_UID.1	NO