netForensics

netForensics Version 3.1.1 With Point Update 45149 Security Target
March 8, 2005
Document No. F2-0305-003

COACT, Inc.
Rivers Ninety Five
9140 Guilford Road, Suite G
Columbia, MD 21046-2587

Phone: 301-498-0150

Fax: 301-498-0855

COACT, Inc. assumes no liability for any errors or omissions that may appear in this document.

DOCUMENT INTRODUCTION

Prepared By:	Prepared For:
COACT, Inc. 9140 Guilford Road, Suite G Columbia, Maryland 21046-2587	netForensics, Inc. 200 Metroplex Drive Edison, NJ 08817

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the netForensics Version 3.1.1 With Point Update 45149, a Security Information Management system. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

REVISION HISTORY

Rev	Description
	March 8, 2005: Initial Release of final document

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS LIST

CC	Common Criteria
EAL2	Evaluation Assurance Level 2
IT	Information Technology
JDBC	Java DataBase Connectivity
nFTP	netForensics Transport Protocol
NIAP	National Information Assurance Partnership
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

CHAPTER 1

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the netForensics Version 3.1.1 With Point Update 45149 Security Information Management (SIM) product. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 2.1*, the ISO/IEC JTC 1/SC27, *Guide for the Production of PPs and STs, Version 0.9* and all National Information Assurance Partnership (NIAP) and international interpretations through September 17, 2003. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

This section provides identifying information for the netForensics Version 3.1.1 With Point Update 45149 Security Target by defining the Target of Evaluation (TOE).

1.1.1 Security Target Name

netForensics Version 3.1.1 With Point Update 45149 Security Target

Initial release

Dated March 8, 2005

1.1.2 TOE Reference

netForensics Version 3.1.1 With Point Update 45149

1.1.3 Security Target Evaluation Status

This ST is currently under evaluation.

1.1.4 Evaluation Assurance Level

Assurance claims conform to EAL2 (Evaluation Assurance Level 2) from the *Common Criteria for Information Technology Security Evaluation, Version 2.1*.

1.1.5 Keywords

Security Information Management, SIM, Network, Security, IDS

1.2 TOE Overview

This Security Target defines the requirements for the netForensics v3.1.1 With Point Update 45149. The netForensics v3.1.1 With Point Update 45149 product is a Security Information Management (SIM) tool. It integrates with third-party security devices, monitoring or protecting a target network, to collect and analyze security relevant information. netForensics v3.1.1 With Point Update 45149 makes it easy to understand the entire threat the network is under by aggregating events.

1.2.1 Security Target Organisation

Chapter 1 of this ST provides introductory and identifying information for the TOE.

Chapter 2 describes the TOE, its architecture, and provides some guidance on its use.

Chapter 3 provides a security environment description in terms of assumptions, threats and organisational security policies.

Chapter 4 identifies the security objectives of the TOE and of the Information Technology (IT) environment.

Chapter 5 provides the TOE functional and assurance requirements, as well as requirements on the IT environment.

Chapter 6 is the TOE Summary Specification, a description of the functions provided by the netForensics Version 3.1.1 With Point Update 45149 product to satisfy the security functional and assurance requirements listed in chapter five.

Chapter 7 identifies claims of conformance to registered Protection Profiles (PP).

Chapter 8 provides references to rationale for the security objectives, requirements, TOE summary specification and PP claims.

1.3 Common Criteria Conformance

This security target is compliant with the *Common Criteria for Information Technology Security Evaluation, Version 2.1*, functional requirements (Part 2 extended) conformant, assurance requirements (Part 3) conformant for EAL2, and all National and International Interpretations through September 17, 2003.

1.4 Protection Profile Conformance

The netForensics Version 3.1.1 With Point Update 45149 does not claim conformance to any registered Protection Profile.

1.5 Document Conventions

The CC defines four operations on security functional requirements. The font conventions below identify the conventions for the operations defined by the CC.

Assignment: **indicated with bold text**

Selection: indicated with underlined text

Refinement: ***indicated with bold text and italics***

Iteration: indicated with typical CC requirement naming followed by a number in parenthesis for each iteration (e.g., FMT_MOF.1 (1))

CHAPTER 2

2. TOE Description

This section provides the context for the TOE evaluation by identifying the product type and describing the evaluated configuration. Also, it provides an overview of the architecture and distinguishes the physical and logical boundaries of the TOE.

2.1 Overview

The netForensics V3.1.1 With Point Update 45149 product is a Security Information Management (SIM) tool in that it collects and analyzes information from Security Devices deployed in a network and provides users with tools for viewing and evaluating the collective state of security.

netForensics collects, normalizes, and aggregates data from a number of third-party Security Devices. Users are able to monitor the collected data in real-time at differing levels of granularity and aggregation through pre-defined views. A wide-range of canned reports, queries, and drilldowns are provided to support forensics, analysis, and risk assessment.

2.2 Operational Environment Overview

As depicted in Figure 1 the following components comprise the netForensics operational environment:

A) nF SIM Desktop

B) nF Security Portal

C) nF WebServer

D) nF Master Engine

E) nF Provider

F) nF Correlation Engine

G) nF Engine

H) Database

I) nF Agents

J) Security Devices

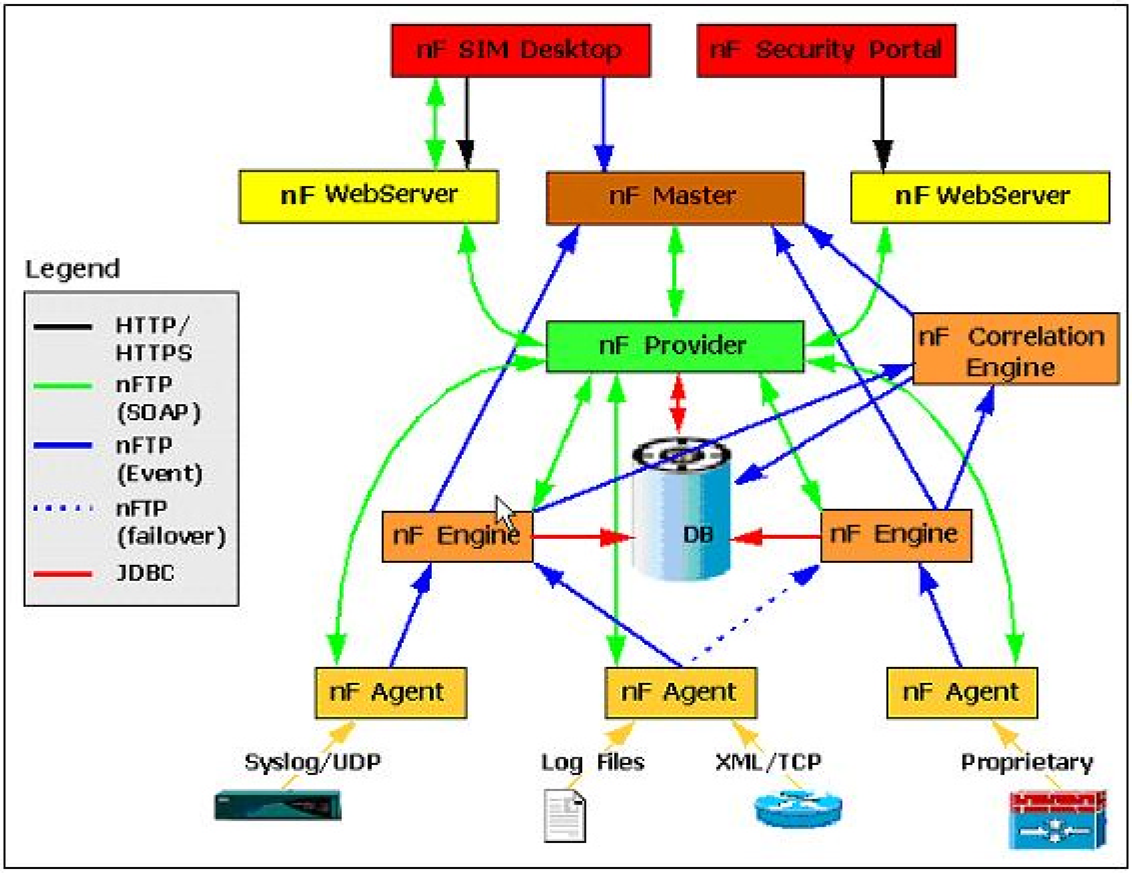

Figure 1 - netForensics Architecture

Starting from the bottom of the figure are various third-party systems that are referred to as Security Devices of the monitored network and systems. These devices can be hardware units like firewalls, software applications like intrusion detection systems (IDS), or operating systems' log files. The Security Devices are not part of the TOE.

Next up are the nF Agents. The nF Agents collect, parse, and normalize the data from the various Security Devices or applications into a standard netForensics XML event schema. This standardized data is referred to as SIM Data, and once created it is pushed upstream to the next nF component.

Next up in Figure 1, the nF Engine performs additional analysis such as event aggregation before forwarding the SIM Data to the nF Master.

The nF Correlation Engine is an add-on product that performs correlation of events from multiple Security Devices. This component is not required for the TOE to function properly, and is not included in this evaluation.

The nF Master is responsible for collecting all of the SIM Data in an installation, maintaining state for analysis, updating real-time GUI components and applying display filters. The nF Master provides real-time data feeds, aggregated from multiple nF Engines, to the nF SIM Desktop clients.

The database used is the Oracle 9i (this component is not included in the TOE).

The nF Provider provides database services to all the registered netForensics components. These include reporting, administration, configuration, master data change (MDC) notification services, and access to the SIM Knowledgebase. The SIM Knowledgebase is pre-defined mappings for Security Device events and patterns of malicious activity.

The nF WebServer acts as the HTTP provider for nF SIM Desktop and nF Security Portal.

The nF SIM Desktop is a Java application that is deployed with the Java Web-Start technology. Whereas, the nF Security Portal is a Web application that provides System Analysts and Administrators with reports and other event review tools.

The nF SIM Desktop interface allows complete policy management for the entire installation including management of user profiles, device profiles, alarms, events, certificates, notification, filtering, agent configuration, and server configuration.

The nF SIM Desktop and nF Security Portal serve as the user interface for two types of users, System Analysts and Administrators. System Analysts can review event data for certain predefined Security Devices as configured by an Administrator. Administrators have the ability to set access rights to System Analysts as well as configure all the components of the system.

2.3 netForensics Deployment

netForensics can be deployed in different modes. A full deployment has all netForensics components installed on the same server. Alternatively the various components can be distributed across multiple servers. The table below summarizes the operating system and application requirements for each TOE component.

Table 1 - Software Requirements

Component	Operating System/Application Requirements
nF Engine	Red Hat Linux 7.1 (Kernel 2.4.9), Solaris 8
nF Master	Red Hat Linux 7.1 (Kernel 2.4.9), Solaris 8
nF WebServer	Red Hat Linux 7.1 (Kernel 2.4.9), Solaris 8
nF Provider	Red Hat Linux 7.1 (Kernel 2.4.9), Solaris 8
nF Security Portal	Red Hat Linux 7.1 (Kernel 2.4.9), Solaris 8
nF Agent	Red Hat Linux 7.1 (Kernel 2.4.9) Sun Solaris 8 Microsoft 2000 Sever/Advanced Server (SP2)
nF SIM Desktop	Java Virtual Machine, Java Web Start 1.2, Java 2 Runtime Environment Standard Edition 1.4.1 or higher

Specific hardware requirements must also be addressed depending on the operating system in use and the component support. The processor requirements are as follows:

A) Red Hat Linux: Intel Pentium III 733 MHz (Server class)

B) Solaris: UltraSPARC-IIi 444 MHz (Server class)

2.4 Physical Boundary

Figure 1 above illustrates the physical boundary of the TOE. Each of the components in the figure that are named with an "nF" is a component of the TOE, except for nF Correlation Engine (a separate add-on product not included in the evaluation). The figure also illustrates the interfaces between each of the TOE components and third party applications and devices. This includes the Database and Security Devices.

The TOE does not include the Security Devices from which data is collected, the operating system hosting any netForensics component, the network, encrypted communications software, the database, or the nF Correlation Engine.

2.5 Logical Boundary

The logical boundary of the TOE is composed of the security functionality described in the following sections.

2.5.1 Security Audit

Actions taken by System Analysts generate audit records. These records contain the date, time, event type, identity of the analyst, and outcome of the action. Only the Administrator has the ability to review and clear these records.

2.5.2 System Analysts' Access Policy

The availability of SIM Data for monitoring and reporting depends on the mappings between System Analysts and Security Devices, because all SIM Data derives from Security Devices. These subjects and objects are mapped by an Administrator to limit the read access System Analysts have to the SIM Data. The Security Devices can be grouped to facilitate complicated or large mappings. The types of groups are Asset Groups, Device Groups and Business Units. For example, a Business Unit can be based on organization, customer, geography, function, etc.

2.5.3 Identification and Authentication

netForensics supports two types of users. An Administrator who has complete control over all aspects of configuration and TSF Data, and a System Analyst whose access is limited to SIM Data from specific Security Devices. Both user interfaces, the nF SIM Desktop and the nF Security Portal, require users to identify and authenticate before accessing.

2.5.4 Administration

The netForensics administration user interface, accessible through the nF SIM Desktop, provides Administrators with the ability to view and centrally manage all users, System Analysts' Access Rights, Device Integration Policies, and Event Analysis Policies. System Analysts' Access Rights dictates which System Analysts can view System Data from which Security Devices. Device Integration Policies are a mapping of Security Device events to nF Alarms. And, Event Analysis Policies are the rules that define the aggregation performed by the nF Engine.

2.5.5 Security Information Management

The nF Agents collect event messages from supported security devices and parse them into normalized SIM Data in accordance with a Device Integration Policy. The normalized events are passed to the nf Engine which performs aggregation analysis across all of the supported Security Devices in accordance with an Event Analysis Policy. The nf Master collects all of the SIM Data from the nF Engines and updates real-time GUI components.

Users are able to monitor the collected data at differing levels of granularity and aggregation through pre-defined views.

CHAPTER 3

3. Security Environment

This chapter identifies the following:

A) IT related threats countered by the TOE and the environment.

B) Significant assumptions about the TOE's operational environment.

C) Organisational security policies for the TOE as appropriate.

Using the above listing, this chapter identifies assumptions (A), threats countered by the TOE (T), threats countered by the operational environment (TE), and organisational security policies (P).

3.1 Threats

The threats identified in the following subsections are addressed by the TOE and IT environment, respectively. For the threats below, attackers are assumed to be of low attack potential.

3.1.1 Threats Addressed by the TOE

T.UNAUTH An unauthorized user accesses the TSF through the TOE's administrative interface.

T.USER_ACC An authorized System Analyst accesses TSF or TSF Data beyond their privilege.

T.ATTACK An attacker directs malicious network traffic against the network monitored by the TOE.

T.INADVERT An individual inadvertently performs some action detected as suspicious by a Security Device the TOE monitors.

T.NOACCNT An authorized System Analyst performs a malicious action.

3.1.2 Threats Addressed by the IT Environment

TE.TAMPER Non-TSF processes on the hosting platforms interfere with the execution of the TSF or the integrity of the TSF data.

TE.COMM An attacker views or modifies communications between TOE components or communications to the nF Security Portal.

3.2 Assumptions

Assumptions are ordered into three groups. They are personnel assumptions, physical environment assumptions, and IT environment assumptions. Personnel assumptions describe characteristics of personnel who are relevant to the TOE. Physical environment assumptions describe characteristics of the non-IT environment that the TOE is deployed in. IT environment assumptions describe the technology environment that the TOE is operating within.

3.2.1 Personnel Assumptions

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

A.PLATFORM The platforms used to host the TOE components will be installed and configured by an administrator and will conform to the specifications listed in Table 1.

A.INSTALL The hardware, operating systems, and software required to support the TOE will be installed and configured by an administrator in conformance with the installation guides.

A.PROTECTED Administrators will ensure that proper firewall and network controls are in place to prevent un-trusted and unknown source network hosts from sending events to the nF Agents.

A.COMPATIBLE Administrators will ensure that Security Devices sending events to the TOE are compatible with the TOE.

3.2.2 Physical Environment Assumptions

A.ENVIRON The TOE will be located in an environment that provides physical security, uninterruptible power, air conditioning, and all other conditions required for reliable operation of the hardware.

3.2.3 Connectivity Assumptions

None

3.3 Organisational Security Policies

None

CHAPTER 4

4. Security Objectives

The objectives identified in the following subsections ensure that all the threats listed in chapter three are addressed by the TOE and the operating environment, respectively.

4.1 Security Objectives for the TOE

The following are the IT security objectives for the TOE:

O.AUTH The TOE must require users to authenticate in order to access the administrative interface.

O.USER_ACC The TOE must restrict authorized users to the TSF and TSF Data that are within the respective user's privilege.

O.COLLECT The TOE must collect, normalize, aggregate, and filter SIM Data.

O.ANALYZE The TOE must analyze and aggregate, and makes the SIM Data and summaries available to the user via views , reports, and alarms.

O.AUDIT The TOE must record all actions of System Analysts and Administrators and changes to User Account Profiles.

O.MANAGE The TOE must provide a set of functions that support effective configuration of the System Analysts' Access Rights, Device Integration Policies, and Event Analysis Policies.

4.2 Security Objectives for the Environment

The following are the IT security objectives for the Environment:

OE.NOTAMPER The IT Environment will provide dedicated platforms to host the TOE.

OE.COMSEC The IT Environment must protect the communications between components of the TOE and communications received by the nF Security Portal from disclosure and modification.

OE.TIMESTAMP The IT Environment must provide a reliable timestamp for use by the TOE.

OE.AUDITSTORE The IT Environment must provide audit and SIM data storage capabilities for use by the TOE.

The non-IT security objectives listed below are to be satisfied without imposing technical requirements on the TOE. Thus, they will be satisfied through application of procedural or administrative measures.

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

OE.PLATFORM The platforms used to host the TOE components will be installed and configured by an administrator and will conform to the specifications listed in Table 1.

OE.INSTALL The hardware, operating systems, and software required to support the TOE will be installed and configured by an administrator in conformance with the installation guides.

OE.ENVIRON The TOE will be located in an environment that provides physical security, uninterruptible power, air conditioning, and all other conditions required for reliable operation of the hardware.

OE.PROTECTED The administrators will ensure that the TOE will be protected via appropriate firewall implementation from un-trusted and unknown source network hosts sending events.

OE.COMPATIBLE The administrators will ensure that the Security Devices sending events to the TOE are compatible with the TOE.

4.3 Rationale for IT Security Objectives

This section provides the rationale that all IT security objectives address threats against the TOE or the Environment.

O.AUTH Addresses T.UNAUTH. By requiring users to authenticate before accessing the TOE, attackers without administrative accounts cannot access the administrative interface of the TOE.

O.USER_ACC Addresses T.USER_ACC. By requiring the TOE to restrict authorized users to TSF and TSF Data within their privilege, the threat of users operating beyond their privilege is mitigated.

O.COLLECT Addresses T.ATTACK and T.INADVERT. By requiring the TOE to collect, normalize, aggregate, and filter SIM Data, the TOE has sufficient data from which to detect malicious activity.

O.ANALYZE Addresses T.ATTACK and T.INADVERT. By requiring the TOE to analyze, aggregate, present data to users, and generate alarms, the TOE has the ability to identify malicious activity and make authorized users of the TOE aware of such activity.

O.AUDIT Addresses T.NOACCNT. By requiring the TOE to record the actions of System Analysts, malicious activity can be tracked to individuals.

O.MANAGE Addresses T.USER_ACC, T.ATTACK, and T.INADVERT. By requiring the TOE to facilitate ongoing configuration of the Access Control Policy, Device Integration Policies, and Event Analysis Policies authorized users can better mitigate the threats listed above by focusing the policies on site-specific concerns.

The objectives below are levied on the environment.

OE.NOTAMPER Addresses TE.TAMPER. By requiring the IT Environment to have dedicated platforms for use by the TOE, there will be no processes to interfere with the execution of the TSF.

OE.COMSEC Addresses TE.COMM. By requiring IT Environment to protect the communications between TOE components and communications to the nF Security Portal, the threat of disclosure and modification of those communications is mitigated.

OE.TIMESTAMP Addresses T.ATTACK, T.INADVERT, and T.NOACCNT. By providing a reliable timestamp for use by the TOE, the IT environment helps to correctly identify records. These records include auditing and SIM Data, therefore all of the threats countered by keeping these records are also mitigated.

OE.AUDITSTORE Partially addresses T.ATTACK, T.INADVERT, and T.NOACCNT. The audit and SIM data storage capabilities permit the TOE to analyze and review the information contained in the records.

Table 2 - Mappings for IT Security Objectives to Threats

	T.UNAUTH	T. USER_ACC	T.ATTACK	T. INADVERT	T. NOACCNT	TE.TAMPER	TE.COMM
O.AUTH	X						
O.USER_ACC		X					
O.COLLECT			X	X			
O.ANALYZE			X	X			
O.AUDIT					X		
O.MANAGE		X	X	X			
OE.NOTAMPER						X	
OE.COMSEC							X
OE.TIMESTAMP			X	X	X		
OE.AUDITSTORE			X	X	X		

4.4 Rationale for Non-IT Security Objectives for the Environment

This section provides the rationale that all non-IT security objectives for the environment address threats or assumptions.

OE.NOEVILADMIN Addresses A.NOEVILADMIN by claiming the administrators are not careless, negligent, or hostile, and they follow guidance as required by A.NOEVILADMIN.

OE.PLATFORM Addresses A.PLATFORM by claiming the hosting platforms will conform to guidance specifications, as required by A.PLATFORM.

OE.INSTALL	Addresses A.INSTALL by claiming the hardware, operating systems, and software require to support the TOE conform to guidance, as required by A.INSTALL.
OE.ENVIRON	Addresses A.ENVIRON by claiming the TOE will be located in an physical environment suitable for the operation of computer equipment A.ENVIRON is addressed.
OE.PROTECTED	Addresses A.PROTECTED by requiring the administrators to implement the network with firewall protection from unwanted traffic to the TOE.
OE.COMPATIBLE	Addresses A.COMPATIBLE by requiring the administrators to use compatible Security Devices when sending events to the TOE.

Table 3 - Mappings for Assumptions to Security Objectives for the Environment

	A. NOEVILADMIN	A. PLATFORM	A. INSTALL	A. ENVIRON	A.PROTECTED	A.COMPATIBLE
OE. NOEVILADMIN	X					
OE. PLATFORM		X				
OE. INSTALL			X			
OE. ENVIRON				X		
OE.PROTECTED					X	
OE.COMPATIBLE						X

CHAPTER 5

5. IT Security Requirements

This section contains the security requirements that are relevant to the TOE. These requirements consist of functional components from Part 2 of the CC as well as explicitly stated requirements, and assurance components from Part 3 of the CC. Any SFR that is marked up by ***-NIAP-XXXX***, is to be considered an explicitly stated requirement. These SFRs correspond with SFRs in the Common Criteria for which a National Information Assurance Partnership (NIAP) interpretation exists. Also, SFRs beginning with "SIM" are explicitly stated SFRs.

This section also contains the Strength of Function claim and corresponding rationale for components that require such a claim.

Table 4 - Security Functional Requirements

Security Functional Requirements of the TOE	
FAU_GEN.1	Audit Data Generation
FAU_SAR.1	Audit Review
FDP_ACC.1	Subset Access Control
FDP_ACF.1	Security Attribute Based Access Control
FIA_UAU.2	User Authentication Before any Action
FIA_UID.2	User Identification Before any Action
FMT_MSA.1	Management of Security Attributes
FMT_MSA.3	Static Attribute Initialisation
FMT_MTD.1	Management of TSF Data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
SIM_COL.1	SIM Data Collection
SIM_ANL.1	SIM Data Analysis
SIM_RCT.1	Analyser React
SIM_ASR.1	Administrator SIM Data Review
SIM_SSR.1	System Analyst SIM Data Review
Security Functional Requirements of the IT Environment	
FAU_STG.1	Protected Audit Trail Storage
FPT_ITT.1	Basic Internal TSF Data Transfer Protection
FPT_SEP.1	TSF Domain Separation
FPT_STM.1	Reliable Time Stamps
FTP_TRP.1	Trusted Path
SIM_STG.1	Protected SIM Data Storage

5.1 Security Functional Requirements of the TOE

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

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 actions of System Analysts**.

FAU_GEN.1.2-***NIAP-0407*** 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 ***(if applicable)***, 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, **no other information.**

Dependencies: FPT_STM.1 Reliable Time Stamps.

5.1.1.2 FAU_SAR.1 Audit Review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide **Administrators** with the capability to read **all data** 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.

Dependencies: FAU_GEN.1 Audit Data Generation.

5.1.2 User Data Protection (FDP)

5.1.2.1 FDP_ACC.1 Subset Access Control

Hierarchical to: No other components.

FDP_ACC.1.1 The TSF shall enforce the **System Analysts' Access Policy** on **System Analysts and SIM Data.**

Dependencies: FDP_ACF.1 Security Attribute Based Access Control.

5.1.2.2 FDP_ACF.1 Security Attribute Based Access Control

Hierarchical to: No other components.

FDP_ACF.1.1-***NIAP-0416*** The TSF shall enforce the **System Analysts' Access Policy** to objects based on ***the following:*** **the identity of the System Analyst and the source Security Device of the SIM Data.**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

Access is allowed if the System Analyst is on the access list for the source of the SIM Data.

FDP_ACF.1.3-***NIAP-0407*** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

None.

FDP_ACF.1.4-***NIAP-0407*** The TSF shall explicitly deny access of subjects to objects based on the ***following rules***:

None.

Dependencies: FDP_ACC.1 Subset Access Control,

FMT_MSA.3 Static Attribute Initialisation.

5.1.3 Identification and Authentication (FIA)

5.1.3.1 FIA_UAU.2 User Authentication Before any Action

Hierarchical to: FIA_UAU.1 Timing of Authentication.

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.

Dependencies: FIA_UID.1 Timing of Identification.

5.1.3.2 FIA_UID.2 User Identification Before any Action

Hierarchical to: FIA_UID.1 Timing of Identification.

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.

Dependencies: No dependencies.

5.1.4 Security Management (FMT)

5.1.4.1 FMT_MSA.1 Management of Security Attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the **System Analysts' Access Policy** to restrict the ability to query, modify, or delete the security attributes **System Analysts' Access Rights** to **the Administrator**.

Dependencies: [FDP_ACC.1 Subset Access Control or

FDP_IFC.1 Subset Information Flow Control],

FMT_SMR.1 Security Roles.

5.1.4.2 FMT_MSA.3 Static Attribute Initialisation

Hierarchical to: No other components.

FMT_MSA.3.1-***NIAP-0442*** The TSF shall enforce the **System Analysts' Access Policy** to provide restrictive default values for ***the following*** security attributes that are used to enforce the SFP***:* System Analysts' Access Rights.**

FMT_MSA.3.2-***NIAP-0442*** The TSF shall allow the **Administrator** to specify alternative initial values to override the default values ***for these attributes*** when an object or information is created.

Dependencies: FMT_MSA.1 Management of Security Attributes,

FMT_SMR.1 Security Roles.

5.1.4.3 FMT_MTD.1 Management of TSF Data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to query, modify, or delete the **Device Integration Policies and the Event Analysis Policies** to **the Administrator**.

Dependencies: FMT_SMR.1 Security Roles.

5.1.4.4 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

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

a) configuration of the System Analysts' Access Policy,

b) configuration of the Device Integration Policies,

c) and configuration of the Event Analysis Policies.

Dependencies: No dependencies.

5.1.4.5 FMT_SMR.1 Security Roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles **Administrator and System Analyst**.

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

Dependencies: FIA_UID.1 Timing of Identification.

5.1.5 Security Information Management Requirements (SIM)

5.1.5.1 SIM_COL.1 SIM Data Collection

SIM_COL.1.1 The TSF shall be able to collect events from the Security Devices for which the TOE has a Device Integration Policy.

SIM_COL.1.2 The TSF shall enforce the Device Integration Policies to collect and record the normalized alarm code, severity, date, time, source IP, username, and the count of events collapsed into one SIM Event (if applicable).

5.1.5.2 SIM_ANL.1 SIM Data Analysis

SIM_ANL.1.1 The TSF shall enforce the Event Analysis Policies to perform aggregation on all SIM Data received. These policies can be based on date, time, and type of event.

SIM_ANL.1.2 The TSF shall enforce the Event Analysis Policies to record within each analytical result at least the following information: date and time of the result and type of result.

5.1.5.3 SIM_RCT.1 Analyser React

SIM_RCT.1.1 The TSF shall enforce the Event Analysis Policies to specify event instance thresholds, create new SIM Events when the specified threshold of normalized alarm instances has been reached, specify alarm destinations, and send alarms via email, pager, SNMP trap, AHD Call request, and AHD Trouble Ticket to specified destinations.

5.1.5.4 SIM_ASR.1 Administrator SIM Data Review

SIM_ASR.1.1 The TSF shall provide Administrators with the capability to read all data from the SIM Data.

SIM _ASR.1.2 The TSF shall provide the SIM Data in a manner suitable for the user to interpret the information.

5.1.5.5 SIM_SSR.1 System Analyst SIM Data Review

SIM _SSR.1.1 The TSF shall provide System Analysts with the capability to read only SIM Data from Security Devices allowed to them by the SIM Data Access Policy.

SIM _SSR.1.2 The TSF shall provide the SIM Data in a manner suitable for the user to interpret the information.

5.2 Security Functional Requirements of the IT Environment

5.2.1 Security Audit (FAU)

5.2.1.1 FAU_STG.1 Protected Audit Trail Storage

Hierarchical to: No other components.

FAU_STG.1.1-***NIAP-0422*** The ***IT Environment*** shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2-***NIAP-0423*** The ***IT Environment*** shall be able to <u>prevent</u> ***unauthorised*** modifications to the audit records ***in the audit trail***.

Dependencies: FAU_GEN.1 Audit Data Generation.

5.2.2 Protection of the TSF (FPT)

5.2.2.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

Hierarchical to: No other components.

FPT_ITT.1.1 The IT Environment shall protect TSF data from <u>disclosure, modification</u> when it is transmitted between separate parts of the TOE.

Dependencies: No dependencies.

5.2.2.2 FPT_SEP.1 TSF Domain Separation

Hierarchical to: No other components.

FPT_SEP.1 The ***IT Environment*** shall maintain a security domain for ***the TOE's*** own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The ***IT Environment*** shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

5.2.2.3 FPT_STM.1 Reliable Time Stamps

Hierarchical to: No other components.

FPT_STM.1.1 The ***IT Environment*** shall be able to provide reliable time-stamps for ***the TOE's*** use.

Dependencies: No dependencies.

5.2.3 Trusted Path/Channels (FTP)

5.2.3.1 FTP_TRP.1 Trusted Path

Hierarchical to: No other components.

FTP_TRP.1.1 The ***IT environment*** shall provide a communication path between ***the nF Security Portal*** and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2 The ***IT environment*** shall permit remote users to initiate communication via the trusted path.

FTP_TRP.1.3 The ***IT environment*** shall require the use of the trusted path for initial user authentication **and subsequent access to the nF Security Portal**.

Dependencies: No dependencies.

5.2.4 Security Information Management Requirements (SIM)

5.2.4.1 SIM_STG.1 Protected SIM Data Storage

SIM_STG.1.1 The TSF shall protect the stored SIM Data from unauthorised deletion.

SIM_STG.1.2 The TSF shall protect the stored SIM Data from unauthorised modification.

5.3 Security Assurance Requirements of the TOE

The TOE meets the assurance requirements for EAL2. These requirements are summarised in the table below.

Table 5 - Assurance Requirements

Assurance Class	Component ID	Component Title
Configuration Management	ACM_CAP.2	Configuration Items
Delivery and Operation	ADO_DEL.1	Delivery Procedures

Assurance Class	Component ID	Component Title
Delivery and Operation	ADO_IGS.1	Installation, Generation, and Start-Up Procedures
Development	ADV_FSP.1	Informal Functional Specification
Development	ADV_HLD.1	Descriptive High-Level Design
Development	ADV_RCR.1	Informal Correspondence Demonstration
Guidance Documents	AGD_ADM.1	Administrator Guidance
Guidance Documents	AGD_USR.1	User Guidance
Tests	ATE_COV.1	Evidence of Coverage
Tests	ATE_FUN.1	Functional Testing
Tests	ATE_IND.2	Independent Testing - Sample
Vulnerability Assessment	AVA_SOF.1	Strength of TOE Security Function Evaluation
Vulnerability Assessment	AVA_VLA.1	Developer Vulnerability Analysis

5.4 Strength of Function Claim of the TOE

The claimed minimum strength of function for the TOE is SOF-basic.

The only probabilistic or permutational mechanism in the TOE is the password mechanism used to authenticate users. The SFR that specifies this mechanism is FIA_UAU.2.

5.5 Rationale for TOE Objectives Coverage

This section provides the rationale that all TOE Objectives have been met by the Security Functional Requirements levied on the TOE.

O.AUTH Satisfied by FIA_UAU.2 and FIA_UID.2. By requiring the TOE to identify and authenticate users before any action with FIA_UID.2 and FIA_UAU.2, respectively, the objective to require users to authenticate before any action is met.

O.USER_ACC Satisfied by FDP_ACC.1, FDP_ACF.1, FAU_SAR.1, FMT_MSA.1, FMT_MSA.3, and FMT_MTD.1. By requiring the TOE restrict System Analysts' access to SIM Data by enforcing the System Analysts' Access Policy with FDP_ACC.1 and by defining that policy with FDP_ACF.1, and by requiring that only Administrators have the ability to access other TSF and TSF Data with FAU_SAR.1, FMT_MSA.1, FMT_MSA.3, and

	FMT_MTD.1, the objective to restrict users to TSF and TSF Data within their privilege is met.
O.COLLECT	Satisfied by SIM_COL.1. By requiring the TOE collect SIM Data from registered Security Devices, the objective for collection is met.
O.ANALYZE	Satisfied by SIM_ANL.1, SIM_RCT.1, SIM_ASR.1, and SIM_SSR.1. By requiring the TOE to analyze SIM Data with SIM_ANL.1, to send alarms with SIM_RCT.1, and to allow user review with SIM_ASR.1 and SIM_SSR.1, the objective to analyze and present the data to TOE users is met.
O.AUDIT	Satisfied by FAU_GEN.1 and FAU_SAR.1. By requiring the TOE to generate audit records for actions taken by the System Analysts with FAU_GEN.1 and to allow audit review by an Administrator with FAU_SAR.1, the objective to provide audit and review of System Analysts actions is met.
O.MANAGE	Satisfied by FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1. By requiring the TOE to allow the Administrator to configure the System Analysts' Access Rights with FMT_MSA.1 and FMT_MSA.3, and to configure the Device Integration Policies and Event Analysis Policies with FMT_MTD.1, and by specifying roles and management functions with FMT_SMR.1 and FMT_SMF.1, the objective to provide configuration of those TSF Data is met.

Table 6 - Mappings Between Functional Requirements and Objectives for the TOE

	O.AUTH	O.USER_ACC	O.COLLECT	O.ANALYZE	O.AUDIT	O.MANAGE
FAU_GEN.1					X	
FAU_SAR.1		X			X	
FDP_ACC.1		X				
FDP_ACF.1		X				
FIA_UAU.2	X					
FIA_UID.2	X					
FMT_MSA.1		X				X
FMT_MSA.3		X				X
FMT_MTD.1		X				X
FMT_SMF.1						X
FMT_SMR.1						X

	O.AUTH	O.USER_ACC	O.COLLECT	O.ANALYZE	O.AUDIT	O.MANAGE
SIM_COL.1			X			
SIM_ANL.1				X		
SIM_RCT.1				X		
SIM_ASR.1				X		
SIM_SSR.1				X		

5.6 Rationale for IT Environment Objectives Coverage

This section provides the rationale that all IT Environment Objectives have been met by the Security Functional Requirements levied on the IT Environment.

OE.COMSEC Satisfied by FPT_ITT.1 and FTP_TRP. By requiring the IT environment to prevent modifications to and disclosure of the communications between the components of the TOE with FPT_ITT.1 and with communications to the nF Security Portal with FTP_TRP, the objective to protect communications received by TOE components and the nF Security Portal is met.

OE.NOTAMPER Satisfied by FPT_SEP.1. By requiring the IT Environment to provide a separate domain of execution, it is assured that other processes will not interfere with the execution of the TSP, as required by the objective.

OE.TIMESTAMP Satisfied by FPT_STM.1. By requiring the IT Environment to provide a reliable timestamp for the TOE's use the objective is met.

OE.AUDITSTORE Satisfied by FAU_STG.1 and SIM_STG.1. By requiring the IT Environment to provide storage capabilities for audit records and SIM data, the objective is met.

Table 7 - Mappings Between Functional Requirements and Objectives for the IT Environment

	OE.NOTAMPER	OE.COMSEC	OE.TIMESTAMP	OE.AUDITSTORE
FAU_STG.1				X
FPT_ITT.1		X		
FPT_SEP.1	X			

	OE.NOTAMPER	OE.COMSEC	OE.TIMESTAMP	OE.AUDITSTORE
FPT_STM.1			X	
FTP_TRP.1		X		
SIM_STG.1				X

5.7 Rationale for Explicitly Stated Requirements

SIM_COL.1 This requirement specifies collecting proprietary events from Security Devices, understanding and normalizing said events and creating internal SIM Events that contain data from this process. Where this requirement is similar to FAU audit requirements in data collection, it differs by being able to understand proprietary events and normalize them in accordance to a Device Integration Policy. These collection and integration functions are not provided by existing SFRs.

SIM_ANL.1 This requirement specifies the aggregation of SIM Data in accordance with Event Analysis Policies. Where this requirement is similar to FAU audit requirements in data analysis, it differs by being able to aggregate events. This analysis function is not provided by existing SFRs.

SIM_RCT.1 This requirement specifies reactions to SIM Events according to a policy. Where this requirement is similar to FAU audit requirements, it differs by processing analyzed SIM Data. Support for this capability is not provided by existing SFRs.

SIM_ASR.1 This requirement specifies providing the Administrators with the ability to read all SIM Data. This is different from existing SFRs because it is dealing specifically with SIM Data.

SIM_SSR.1 This requirement specifies limited access to SIM Data for System Analysts. This is different from existing SFRs because it is dealing specifically with SIM Data.

SIM_STG.1 This requirement specifies protecting and storing SIM data. This is different from existing SFRs because it is dealing specifically with SIM Data.

5.8 Rationale for Security Assurance Requirements of the TOE

EAL2 was chosen to provide a low to moderate level of independently assured security. The chosen assurance level is consistent with the postulated threat environment. Specifically, that the threat of malicious attacks (being considered of low potential) is not greater than moderate and the product will have undergone a search for obvious flaws.

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 from part 3 of the Common Criteria.

5.9 Rationale for Strength of Function Claim

SOF-basic is defined in CC Part 1 section 2.3 as: "A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential."

Because this ST identifies threat agents with low attack potential, SOF-basic was chosen.

5.10 Rationale for IT Security Requirement Dependencies

The following table lists the claimed TOE and IT Environment security requirements and their dependencies. This section also contains rationale for any dependencies that are not satisfied.

Table 8 - Functional Requirements Dependencies

SFR	Dependencies	Hierarchical To
FAU_GEN.1	FPT_STM.1	None
FAU_SAR.1	FAU_GEN.1	None
FAU_STG.1	FAU_GEN.1	None
FDP_ACC.1	FDP_ACF.1	None
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	None
FIA_UAU.2	FIA_UID.1	FIA_UAU.1
FIA_UID.2	None	FIA_UID.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1	None
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	None
FMT_MTD.1	FMT_SMR.1	None
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	None

SFR	Dependencies	Hierarchical To
SIM_COL.1	None	None
SIM_ANL.1	None	None
SIM_RCT.1	None	None
SIM_ASR.1	None	None
SIM_SSR.1	None	None
SIM_STG.1	None	None
FPT_ITT.1	None	None
FPT_SEP.1	None	None
FPT_STM.1	None	None
FTP_TRP.1	None	None

FIA_UAU.2 and FMT_SMR.1 are dependent upon FIA_UID.1. FIA_UID.2 is hierarchical to FIA_UID.1; therefore this dependency is satisfied.

FMT_MSA.1 requires that either FDP_ACC.1 or FDP_IFC.1 be included. FDP_ACC.1 is included to fulfil this dependency.

CHAPTER 6

6. TOE Summary Specification

6.1 TOE Security Functions

This section describes the security functions implemented by the TOE to meet the TOE SFRs.

6.1.1 Security Audit

The netForensics role, System Analysts, is the general user for the TOE. These users are intended to the actual review of the SIM Data, receive alarms, etc. for the SIM Data that they are responsible and authorised to view. The System Analysts can view the SIM Data and drill down into details of events. They can also generate and print reports.

Each of the actions taken by the System Analyst generates a record containing the date, time, type, identity of the analyst, and outcome of the action. Only the Administrator has the ability to review these records.

The Security Audit function of netForensics meets the following SFRs:

A) FAU_GEN.1

B) FAU_SAR.1

6.1.2 System Analysts' Access Control

The TOE provides the ability to control System Analyst access to SIM Data based on the source of the SIM Data. For example, a System Analyst may be only able to view data from one geographical segment of the network. An Administrator can define the System Analysts' Access Rights. This is simply a table of access rights mapping System Analysts to integrated Security Devices.

An Administrator can define logical groups of devices and assets to facilitate mapping large or complicated policies. The groups available are Asset Groups, Device Groups, and Business Units. For example, a Business Unit can be based on organization, customer, geography, function, etc.

The System Analysts' Access Control function meets the following SFRs:

A) FDP_ACC.1

B) FDP_ACF.1

6.1.3 Identification and Authentication

All users of nF SIM Desktop and nF Security Portal must authenticate by logging in. The login process includes the following steps:

1) enter username and password,

2) login button clicked by user,

3) login validated,

4) upon failure, repeat from step 2.

After the user id and password are successfully validated, the main window is launched.

The Identification and Authentication function of netForensics meets the following SFRs:

A) FIA_UAU.2

B) FIA_UID.2

6.1.4 Administration

The nF SIM Desktop provides Administrators with the ability to view and centrally manage the configuration parameters for all netForensics users and components.

Administrators have general user privileges and can configure or alter netForensics settings and configuration parameters that affect System Analysts, integrate Security Devices, and configure the analysis performed on the SIM Data.

The following detailed options are supported:

A) System Analysts' Access Rights – Under this option Administrators can create a mapping for System Analysts to Security Devices.

B) Event Analysis Policies– This option allows Administrators to change the default settings for the aggregation of SIM Data based on date, time, and type of event.

C) Device Integration Policies –This option allows Administrators to modify the policies governing the integration of the Security Devices. These policies can be based on normalized alarm code, severity, date, time, source IP, username, and the count of events aggregated into an event.

The Administration function of the netForensics meets the following SFRs:

A) FMT_MSA.1

B) FMT_MSA.3

C) FMT_MTD.1

D) FMT_SMF.1

E) FMT_SMR.1

6.1.5 Security Information Management

An nF Agent consists of Protocol Adaptors, Data Processors, and the Device Integration Policy. The Protocol Adaptors communicate with the Security Devices to receive their specific events. The Data Processors take the events streamed by the Protocol Adaptors, apply the Device Integration Policy, normalize, filter, create, and push the nF Events upstream to the nF Engine. As the event stream is collected, the nF Agent will parse and normalize by mapping device alarms to a single nF Alarm. nF Alarms are mapped to nF Categories in a pre populated table. A normalized nF Severity, a number from 1 to 5, is also assigned based on the severity reported by the device, information from the SIM Knowlegebase, and any custom rules specified by the administrator. Events with a severity of 1, 2, and 3 will be marked as LOW priority events and stored in the "lowseverityevent" table. Events with severities of 4 and 5 will be marked as HIGH and stored in the "highseverityevent" table. The use of the event tables improves performance when generating reports.

The manner in which the security messages should be parsed differs depending on the source and is defined by the Administrator via the Device Integration Policies. Specifically, the Administrator defines a mapping between application or device specific events and nF Alarms. The nF Agent's configuration and rule set for parsing application messages are also defined by the Device Integration Policy. The rules are defined using regular expressions. The other mappings are implemented as static tables provided with the product.

The nF Engine processes the collected events in a round robin fashion, aggregates events, saves events to the database, and forwards them to the nF Master for real-time broadcasting. The nF Engine is a multi-threaded server and handles multiple nF Agents at the same time. The nF Engine can be configured to:

A) support the aggregation of events based on customizable rules evaluating device types, instances, alarm ID and other event attributes over specified window of time

B) filter and forward events based on event priority, event severity, alarm category, and alarm id to the Database, nF Master, another nF Engine or external application

C) send notifications via email, pager, SNMP traps, trouble tickets

D) provides for storing dates in the time zones specified in system policies

The nF Master collects nF Events from nF Engines over secure channels and broadcasts events to subscribed users. nF Master is multi-threaded and handles multiple nF Engines at the same time. Events are queued up on a priority basis for parsing and event processing. HIGH priority messages will be given processing preference.

The nF SIM Desktop communicates with the nF Master for real-time SIM Data display and with the nF Provider for all master information and processing of reports. Data can be displayed in the following formats:

A) Device Map – displays the status of business units and devices based on event severity or alarm category.

B) Device Status – displays the event categories and severities from a device

C) Event Console – displays events generated by security devices according to user-defined console filters

In addition users can access the nF Security Portal via a Web interface to view generated reports. A variety of pre-defined device-independent and vendor specific reports are provided to support data mining and user directed analysis. Administrators can schedule reports to be run at a chosen time.

The Security Information Management function meets the following SFRs:

A) SIM_COL.1

B) SIM_ANL.1

C) SIM_RCT.1

D) SIM_ASR.1

E) SIM_SSR.1

6.2 Assurance Measures

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 from part 3 of the Common Criteria.

The following table demonstrates the correspondence between the security assurance requirements listed in Chapter 5 to the developer evidence.

Table 9 - Assurance Correspondence

Component ID	Developer Evidence
ACM_CAP.2	The following Configuration Management procedures are described in documentation: Use of the CM tool for revision control List of configuration items and evidence that they are maintained by the CM tool.
ADO_DEL.1	This documentation includes descriptions of the process used to create distribution copies of the TOE and the procedures used to ensure consistent delivery of the TOE.
ADO_IGS.1	This documentation describes the procedures necessary for secure installation, generation, and start-up of the TOE.
ADV_FSP.1	This documentation provides the purpose and method of use of all external TSF interfaces and completely represent the TSF.
ADV_HLD.1	This documentation describes the high level design. It contains a representation of the TSF in terms of subsystems, and describes the security functions. All subsystem interfaces are identified and the externally visible ones are noted.
ADV_RCR.1	The correspondence between the TOE security functions and the high-level design subsystems is described in this documentation.
AGD_ADM.1	Guidance to administrators is effectively supported by the documentation for this requirement.

Component ID	Developer Evidence
AGD_USR.1	Guidance to non-administrative users is effectively supported by the documentation for this requirement.
ATE_COV.1	This documentation describes the functional tests performed and their results.
ATE_FUN.1	This documentation describes the functional tests performed and their results.
ATE_IND.2	This documentation describes the functional tests performed and their results.
AVA_SOF.1	This documentation includes a strength of function analysis to support the SOF-basic claim. The analysis includes identifying the TOE password space and the probability of a password being compromised.
AVA_VLA.1	This documentation describes the vulnerability analysis performed and the results of the analysis.

6.3 Rationale for TOE Security Functions

The following section provides a rationale showing how each Security Functional Requirement is supported by the security functions enforced by the TOE.

FAU_GEN.1 Is supported by the Security Audit function. This function audits all actions made by System Analyst users. This directly fulfils this SFR.

FAU_SAR.1 Is supported by the Security Audit function. The Security Audit function provides the Administrator the ability to review audit records through the nF SIM Desktop. This directly fulfils this SFR.

FDP_ACC.1 Is supported by the System Analysts' Access Control function. This function names and defines the access control policy and what it is enforced upon. This directly supports this SFR that identifies an access control policy.

FDP_ACF.1 Is supported by the System Analysts' Access Control function. This function names and defines the access control policy and what it is enforced upon. This directly supports this SFR that defines the subjects, objects, and actions of an access control policy.

FIA_UAU.2 Is supported by the Identification and Authentication function. The Identification and Authentication function provides a secure login page to the nF SIM Desktop and nF Security Portal, and requires users to successfully authenticate before allowing them any access to the TOE. This directly fulfils this SFR.

FIA_UID.2 Is supported by the Identification and Authentication function. The Identification and Authentication function provides a secure login page to the nF SIM Desktop and nF Security Portal, and requires users to successfully authenticate before allowing them any access to the TOE. An authenticated user is also an identified user. Therefore, this fulfils this SFR.

FMT_MSA.1 Is supported by the Security Management function. The Security Management function provides the ability for the Administrator to configure the System Analysts' Access Rights. This directly fulfils this SFR.

FMT_MSA.3 Is supported by the Security Management function. The Security Management function specifies that the System Analysts' Access Rights are restrictive by default. This directly fulfils this SFR.

FMT_MTD.1 Is supported by the Security Management function. The Security Management function provides the ability for the Administrator to configure the Allowable Use Policies. This directly fulfils the FMT_MTD.1 requirement.

FMT_SMF.1 Is supported by the Security Management function. The Security Management function provides the ability to configure the System Analysts' Access Policy, the Device Integration Policies, and the Event Analysis Policies. This directly fulfils this SFR.

FMT_SMR.1 Is supported by the Security Management function. The Security Management function provides two system roles, Administrators and System Analysts. This directly fulfils this SFR.

SIM_COL.1 Is supported by the Security Information Management function. This function specifies that the TOE will collect SIM Data from Security Devices that have been integrated with the TOE. This directly fulfils this SFR.

SIM_ANL.1 Is supported by the Security Information Management function. This function specifies that the TOE will aggregate SIM Data. This directly fulfils this SFR.

SIM_RCT.1 Is supported by the Security Information Management function. This function specifies that the TOE will send alarms in accordance with the Event Analysis Policies. This directly fulfils this SFR.

SIM_ASR.1 Is supported by the Security Information Management function. This function specifies that the TOE will provide Administrators with complete review of all SIM Data. This directly fulfils this SFR.

SIM_SSR.1 Is supported by the Security Information Management function. This function specifies that the TOE will provide System Analysts with review of limited SIM Data as specified by the System Analysts' Access Policy. This directly fulfils this SFR.

Table 10 - Mappings Between SFs and SFRs for the TOE

	Security Audit	System Analysts' Access Control	Identification and Authentication	Administration	Security Information Management
FAU_GEN.1	X				
FAU_SAR.1	X				
FDP_ACC.1		X			
FDP_ACF.1		X			
FIA_UAU.2			X		
FIA_UID.2			X		
FMT_MSA.1				X	
FMT_MSA.3				X	
FMT_MTD.1				X	
FMT_SMF.1				X	
FMT_SMR.1				X	
SIM_COL.1					X
SIM_ANL.1					X
SIM_RCT.1					X
SIM_ASR.1					X
SIM_SSR.1					X

6.4 Rationale for Satisfaction of Strength of Function Claim

The claimed minimum strength of function is SOF-basic. The authentication requirement, FIA_UAU.2, contains a permutational function requiring an SOF analysis. It should be noted that there is no distinction between Administrator and System Analyst with respect to FIA_UAU.2. Therefore, only one analysis is presented:

Password space for the TOE users:

Users can set their password through the nF SIM Desktop that communicates with the nF Web Server using TCP/IP. Because of A.ENVIRON, we assume that an attacker does not have access to the machine that is hosting the nF Web Server. Therefore, an attack must go over the network. Based on a typical high-speed Ethernet and experience with brute-force attack engines, a conservative estimated transfer of 5,000 guesses can be made each second (0.0002 seconds/attempt).

The password can contain upper and lower case letters and digits. This provides at 62 distinct characters. Therefore, the password space is calculated as follows (divided by two for average):

Password length: p = 5

Unique characters: c = 62

Seconds per attempt: s = 0.0002

Average length of successful attack in days =

= (s * c^p seconds) / (60 * 60 * 24 seconds per day) / 2

= (0.0002 * 62^5) / (60 * 60 * 24) / 2

= 1 day

Using the approach detailed in the CEM Part 2 Annex B, the values for “Identifying Value” and "Exploiting Value" in Table B.3 for each factor were summed. Given the simplicity of a brute force attack, all the values are 0 except for the Exploiting Value for Elapsed Time (5) and Access to TOE (6) for a total of 11. As shown in Table B.4, values between 10 and 17 indicate the mechanism is sufficient for a SOF Rating of ‘Basic’, resistant to an attack potential of ‘low’.

CHAPTER 7

7. Protection Profile Claims

This chapter provides detailed information in reference to the Protection Profile conformance identification that appears in Chapter 1, Section 1.4 Protection Profile Conformance.

7.1 Protection Profile Reference

This Security Target does not claim conformance to any registered Protection Profiles.

7.2 Protection Profile Refinements

This Security Target does not claim conformance to any registered Protection Profiles.

7.3 Protection Profile Additions

This Security Target does not claim conformance to any registered Protection Profiles.

7.4 Protection Profile Rationale

This Security Target does not claim conformance to any registered Protection Profiles.

CHAPTER 8

8. Rationale

This chapter provides rationale or references to rationale required for this Security Target.

8.1 Security Objectives Rationale

Sections 4.3 - 4.4 provide the security objectives rationale.

8.2 Security Requirements Rationale

Sections 5.5 - 5.10 provide the security requirements rationale.

8.3 TOE Summary Specification Rationale

Sections 6.3 – 6.4 provide the TSS rationale.

8.4 Protection Profile Claims Rationale

This Security Target does not claim conformance to any Protection Profile.