Q1 Labs

QRadar™ V5.1.2

Security Target V 2.0.4

January 30, 2007

Prepared By:

CYGNACOM SOLUTIONS

Suite 5200 West♦7925 Jones Branch Drive♦McLean, VA 22102-3321♦703 848-0883♦Fax 703 848-0960

TABLE OF CONTENTS

Table of Tables and Figures

Table or Figure **Page**

1 Security Target Introduction

1.1 Security Target Identification

TOE Identification: QRadar V5.1.2, with modules Offence Resolution v1.0 and Offence Manager

ST Title: Q1 Labs QRadar v5.1.2 Security Target

ST Version: Version 2.0.4

ST Date: January 30, 2007

Assurance Level: EAL2

Registration: VID10050

Keywords: Intrusion Detection, Intrusion Detection System, Sensor, Scanner, and Analyzer

1.2 Security Target Overview

This Security Target (ST) defines the Information Technology (IT) security requirements for Q1 Labs QRadar v5.1.2 network security monitoring system, with modules Offence Resolution v1.0 and Offence Manager.

The Q1 Labs QRadar v5.1.2 product is an administrator configurable network intrusion detection and response system. Note that the product is also referred to as “QRadar” in this ST.

QRadar collects and process data both from network taps and from event collectors installed on network devices. The product produces security events by real-time event matching and by comparing the collected data to historical flow-based behaviour patterns. The security events are then correlated by the product to produce weighted alerts which are sent to the product users. Note that all QRadar users are trusted and are granted privileges to manage an Enterprise’s network or subnet.

QRadar also can be configured to return a security response to configured network devices, either automatically, or in response to an action taken by an authorized user. By this means, a network device may be reconfigured to isolate a detected network security threat.

QRadar supports the user in manually isolating threats to specific hosts or groups of hosts through customizable views and reports representing network devices, groups of network devices, and collections of data, security events, and alerts.

QRadar includes its own auditing, user identification and authentication, security management, and TSF self protection mechanisms. The security management mechanism specifically supports limiting a user’s access to the data collected from the network.

QRadar’s Offence Resolution v1.0 and Offence Manager modules are product packages that bundle specific user interfaces and product functionality. The Offence Manager module includes the product’s functional and user interface components that support the correlation of security alerts to reduce false positives and association of alerts to security events. The Offence Resolution module includes the product’s functionality and user interface components needed to associate a security event to a network device (or group of network devices) and return a security response to that network device (or devices).

The Target of Evaluation (TOE) is a distributed, software-only TOE. The TOE includes all product components, except those that are installed directly on third party devices. However, product components that are installed directly on third party devices were included in the test configuration as interfaces to the TOE. The product components that are installed on third party network devices are the Device Support Module and the External Event Collector.

In summary, the product components included in the TOE are the QRadar v5.1.2 server software and user interface components, the product modules Offence Resolution v1.0 and Offence Manager software and user interface components, the product's collectors that access network taps, and the interface to the External Event Collector and the Device Support Module.

The TOE is available installed in all-in-one 'Appliance' products, or may be installed by the end-user on a suitable hardware platform.

1.3 Common Criteria Conformance

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 2 from the Common Criteria Version 2.3, ISO/IEC 18405.

1.4 Document Organization

The main sections of an ST are the ST Introduction, Target of Evaluation (TOE) Description, TOE Security Environment, Security Objectives, IT Security Requirements, TOE Summary Specification, and Rationale.

Section 2, TOE Description, describes the product type and the scope and boundaries of the TOE.

Section 3, TOE Security Environment, identifies assumptions about the TOE's intended usage and environment and threats relevant to secure TOE operation.

Section 4, Security Objectives, defines the security objectives for the TOE and its environment.

Section 5, IT Security Requirements, specifies the TOE Security Functional Requirements (SFR), Security Requirements for the IT Environment, and the Security Assurance Requirements.

Section 6, TOE Summary Specification, describes the IT Security Functions and Assurance Measures.

Section 7, Protection Profile (PP) Claims, is not applicable, as this product does not claim conformance to any PP.

Section 8, Rationale, presents evidence that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The Rationale has three main parts: Security Objectives Rationale, Security Requirements Rationale, and TOE Summary Specification Rationale.

Sections 9 and 10 provide acronym definitions and references.

2 TOE Description

The TOE is defined as all Q1 Labs QRadar v5.1.2 product components except the Device Support Module and the External Event Collector, which were included in the test configuration as interfaces to the TOE. The QRadar Engine and Console TOE component is enhanced by the inclusion of the product's Offence Resolution v1.0 and Offence Manager modules. As shown in Figure 2-1, the product components included in the TOE are the QRadar Engine and Console and the QFlow Collector. Each of these is described as follows:

- The QFlow Collector passively collects traffic flows from a network tap and forwards the collected network traffic to the QRadar Engine.
- The QRadar Engine is the core of the product and supports:
    - o the collection, analyses and storage of data gathered by the QFlow Collector and the external event collectors,
    - o the generation and correlation of alerts to security events, filtering of 'false positive' security alerts, population of user interface views, and generation of reports to support the Administrator in identifying and countering network security threats and vulnerabilities,
    - o the automatic return of a security response to configured network devices upon detection of specific security events, and
    - o the auditing of user actions, user identification and authentication, security management, and TSF self protection mechanisms.

  The subcomponents of the QRadar Engine are presented in Section 2.3.1.
- The QRadar Console utilizes pre-analyzed data derived by the QRadar Engine to populate the user interface. The QRadar Console GUI screen includes the Dashboard view, the Offence Manager view, the Offence Resolution view, the Network Surveillance view, and the Reports view.
    - o The Dashboard is a customizable view that appears immediately upon user authentication. It allows the user to monitor the overall network behavior, security and vulnerability posture, top targeted assets, top attackers, and worst and most recent security Offences from one window.
    - o The Offence Manager view supports the user in correlating security alerts to reduce false positives and in associating alerts with security events. .
    - o The Offence Resolution view supports the user in associating a security event to a network device (or group of network devices) and returning a security response to that network device (or devices).
    - o The Network Surveillance view supports the user in monitoring the behavioral profiles of network traffic associated with systems and applications. This is useful to trace the source of alerts and events to specific systems and applications.
    - o The Reports view provides "out of the box" Executive and Operations level reporting capability. Additional customized reports may be defined by the user.

2.1 Product Type

The Q1 Labs QRadar v5.1.2 product is an administrator configurable network intrusion detection and response system.

2.2 Product Description

The product collects and processes data from network taps through the QFlow Collector and from QRadar External Event Collectors installed on network devices. The QRadar External Event Collector was included in the test configuration only as an interface to the TOE. The product produces security

events from the data collected by the QFlow Collector by comparing the data with historical behaviour patterns and by performing real-time event matching through Sentries. The security events generated in this way are then correlated by the product with the event data collected from QRadar Event Collectors and refined so that similar events are grouped into a single weighted alert which is sent to the product users. QRadar provides alerts based on behaviors, anomalies, policies and thresholds.

Upon receiving the weighted alert, the user can selectively decompose it, exposing the associated security events and collected data for further investigation.

The product can be configured to return a security response to configured network devices, either automatically, or in response to an action taken by a user. The built-in security responses are: TCP Resets, ARP Redirection, and the ability to issue commands to network devices such as switches routers and firewalls, but a general interface for passing data and commands to configured network devices is also included. By these means, a network device may be configured to isolate detected network security threats.

The product includes its own auditing, user identification and authentication, security management, and TSF self protection mechanisms. The security management mechanism specifically supports limiting a user's access to the data collected from the network.

No cryptographic functionality is included in the product or the TOE.

The QRadar software included in the TOE is modular and components and subcomponents as identified below in Section 2.3.1. The software can support product configurations where product components are installed on independent platforms. However, in the evaluated configuration the QFlow Collector was installed on one platform, and all other TOE components are installed on a single server.

In addition, the TOE software components are incorporated into the following QRadar 'Appliance' products, which provide the identified QRadar security services on pre-installed and configured servers:

- Appliance # 2101 (Entry-Level 'All in 1" Appliance) – This is an all –in-one box that enables the user to collect "flows" (QFlow) and events.
- Appliance # 2102 (Entry-Level 'All in 1" Appliance) – This is an all –in-one box that includes the same features as #2101 but also includes an Endace copper NIC for greater performance
- Appliance # 3101 (Mid-Level Server Appliance) – This includes the same features as Appliance # 2101 except that there is a larger Storage array and QFlow capability is not configured upon delivery. Event Collecting/Processing is included.
- Appliance # 4101 (High-End Server Appliance) – This includes the same features as Appliance # 3101 except that it has a quad CPU and there is no .QFlow or Event Collecting/Processing capability included.

Appliance # 2101 was tested in the evaluated configuration.

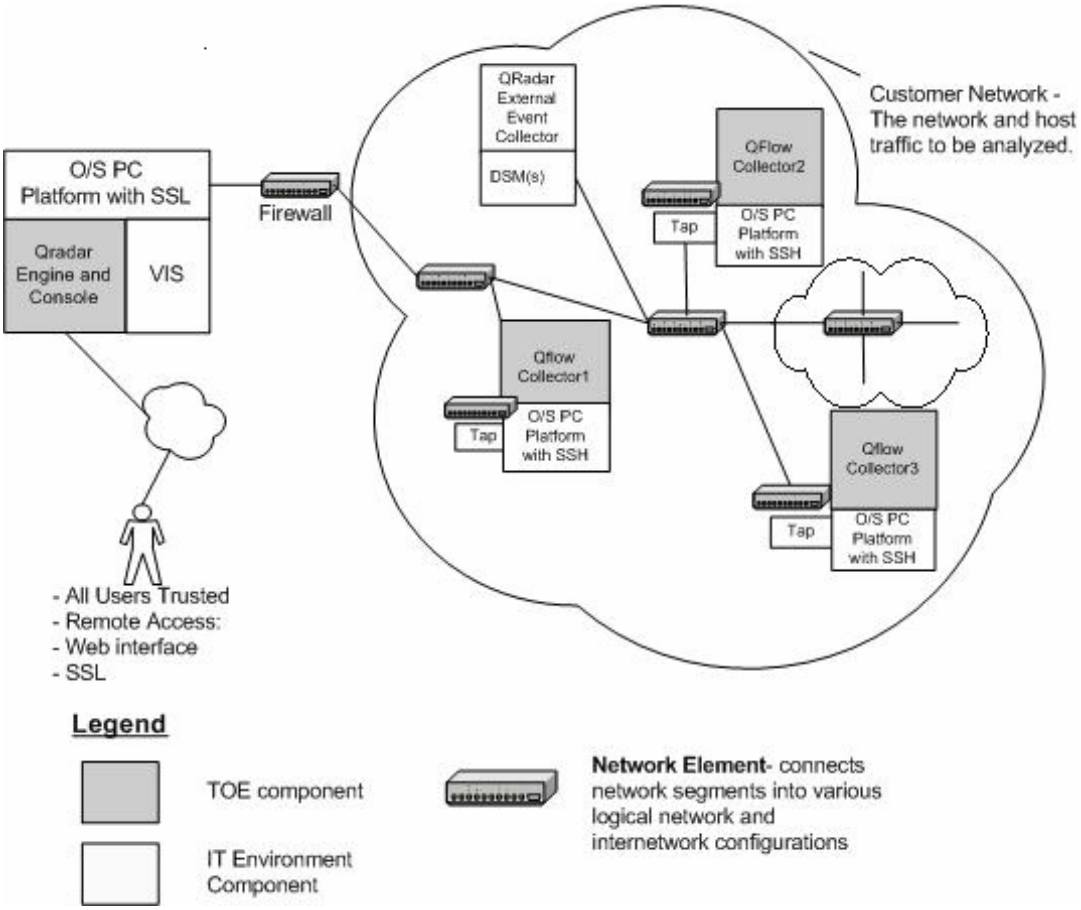

Figure 2-1 QRadar Architecture Diagram and Physical TOE Boundary

Note: In Figure 2-1 the Flow Processor, Classification Engine, Internal Event Collector, External Event Processor, QRadar Console and Magistrate Processing Core TOE subcomponents are shown as the 'QRadar Engine and Console'.

2.3 TSF Physical Boundary and Scope of the Evaluation

2.3.1 The TOE Components

The TOE is defined as Q1 Lab's QRadar v5.1.2 software components QRadar Engine and Console and the QFlow Collector. The exact version of the software components is version 5.1.2. All product components of the TOE are software. QRadar v5.1.2 includes the following product components and subcomponents:

- QFlow Collector(s)
- QRadar Engine and Console
    - Flow Processor
    - Classification Engine
    - Internal Event Collector
    - External Event Processor
    - QRadar Console
    - Magistrate Processing Core

The subcomponents of the QRadar Engine and Console are the Flow Processor, the Classification Engine, Internal Event Collector, Event Processor, QRadar Console, and the Magistrate Processing Core. These subcomponents are referenced in this document in order to add clarity to the description of the operation and function of the product. A brief description of each of these subcomponents follows:

- The **QRadar Flow Processor** collects and consolidates data from one or more QFlow Collector(s) and passes the consolidated data to the Classification Engine.
- The **Classification engine** receives consolidated data from the Flow Processor, and determines if an event should be generated.
- The **Internal Event Collector** of the Event process receives policy and security data emitted internally from the QRadar Classification engine.
- The **External Event Processor** receives the normalized data from the External Event Collector. The External Event Collector is included in the TOE as an interface only.
- The **QRadar Console** includes User access functionality that corresponds with the necessary Security Functionality Requirements.
- The **Magistrate Processing Core** (MPC) is responsible for collecting the events generated internally from the Internal Event Collector and externally from the External Event Processor. It correlates these events and takes actions such as issuing alerts and/or executing automated actions triggered by detected events. It also supports the functionality required to enable the user to investigate alerts and events.

2.3.2 The TOE IT Environment Components

The following are the IT Environment components required for operation of the TOE and to support the TOE's security functions:

- Hardware platform(s): Intel PC Platforms, one for each QFlow Collector, and one for all other TOE components.
- Operating System platform(s): Trustix 2.2 for all product components. The product is also certified to run on Linux Red Hat Enterprise v.4.
- Supporting S/W on the customer network:
  - QRadar External Event Collector and its associated Device Support Modules (DSMs) compatible with the network devices being monitored;
  - 3rd party vulnerability scanning modules such as Nessus
  - QFlow Vulnerability Assessment (VA) Integration Server module providing an interface for the vulnerability scanners.
- Protection of data in transit between the QFlow Collectors and the QRadar server, and between the QRadar Server and the External Event Collector. This can be implemented by physical protection of the network connection between the collectors and the Server, or a virtual LAN such as that supported by cryptographic module(s) such as Open SSL.
- Network or other connectivity:
  - Ethernet network to connect the TOE. Note that the TOE can also be installed on a single platform.
  - Based on customer requirements, connectivity between Network Elements that support a tap for the QFlow Collectors.

2.4 Logical Boundary

The TOE provides the following security features:

- Security Audit
- Identification and Authentication
- Security Management
- Partial TSF Self-Protection
- Intrusion Detection

2.4.1 Security Audit

QRadar provides the ability to audit blocks generated by the TOE and the addition, modification, and deletion of configuration information that specifies the blocks. QRadar is able to associate the auditable events with identified users.

2.4.2 Identification and Authentication

QRadar provides user identification and authentication independent of that provided by the operating system through the use of user identifiers and passwords.

2.4.3 Security Management

QRadar supports the following administrative roles: Administrator, User, and Customer and limits the management of TSF Data to users with the appropriate privileges and network access.

QRadar provides the following security management functionality:

- Management of security management data
- Management of collected event data and collected network data
- Management of CIDR ranges assigned to users
- Management of blocks
- Management of passwords

2.4.4 Partial TSF Self-Protection

QRadar provides for non-bypassability and for protection of the audit data and defense perspective data in conjunction with the operating system platform,

2.4.5 Intrusion Detection

QRadar provides for customer network data collection and processing to create the set of surveillance information. This includes a database of flow information, a set of analysis data, and a database of external event information. The intrusion detection function provides the following capabilities:

- Reads network data in real-time including data from Gigabyte networks
- Allows for amount of payload information to be configured by bytes per Collector.
- Analyzes vulnerability data by correlating the event with the various types of raw data, normalized data, and Offences. As a result, weighted Offence alerts can be generated.
- Provides behavioral and event correlation analysis on surveillance information
- Records results by date, time, and type
- Generates internal events and their associated violations
- Sends alerts based on analysis of defense perspective data

- Provides security responses to block network security threats based on analysis of defense perspective data.
- Generates automatic reports on defense perspective data.
- Provide Administrators and Users the ability to review the defense perspective data they are authorized to view.

2.5 TOE Security Environment

It is assumed that there will be no untrusted users or software on the QRadar server(s).

The TOE environment is one where the potential attacker is unsophisticated, with access to only standard equipment and public information about the product.

The Security Functions provided by the TOE security environment can be categorized as follows:

- **Event and vulnerability data collection on the customer network -** The TOE relies on QRadar IT Environment components on the customer network to collect event data from network devices that produce Netflow, Jflow, and Sflow events through the External Event Collector.
- **Cryptographic Support -** The TOE relies on the IT environment to provide cryptographic support and the cryptographic module which includes OpenSSL for secure data communication over a trusted channel. The TOE does not include any cryptographic functionality, nor does include an interface to any cryptographic functionality.
- **Partial Protection of TSF -** QRadar relies on the underlying platform, OS and hardware, to provide security capabilities for the TOE's protection. These include SFP domain separation, Non-bypassability of the TSP, and a reliable time-stamp. The TOE also relies on the platform to support the protection of the audit and defense perspective data.

3 TOE Security Environment

This section identifies secure usage assumptions and threats to security.

3.1 Assumptions

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

Table 3-1 Assumptions

Item	Assumption	Assumption Description
1.	A.ACCESS	The TOE has access to all the IT security management data and defense perspective data it needs to perform its functions.
2.	A.DYNAMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
3.	A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
4.	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.
5.	A.PASSWD	Authorized users will follow the guidance provided by the TOE documentation for choosing good passwords.
6.	A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
7.	A.PROTCTCOMM	Those responsible for the TOE will ensure the communications between the TOE components are secure via a SSL secure channel.
8.	A.SCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.
9.	A.TRUSTED	There will be no untrusted users of the TOE and no untrusted software loaded on the TOE host platforms.

Application Note: A.PROTCTCOMM provides for a secure communications between the User Web interface and QRadar Server Console, and among the TOE components when operating in a distributed environment (see Figure 2-2).

3.2 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker is unsophisticated, with access to only standard equipment and public information about the product.

The TOE must counter the following threats to security:

Table 3-2 TOE Threats

Item	TOE Threat	TOE Threat Description
1.	T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
2.	T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
3.	T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.

Item	TOE Threat	TOE Threat Description
4.	T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
5.	T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
6.	T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
7.	T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.

Table 3-3 IT System Threats

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

Item	IT Threat	IT Threat Description
8.	T.SCNCFG	Improper security configuration settings may exist in the IT System the TOE monitors.
9.	T.SCNMLC	Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.
10.	T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors.
11.	T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
12.	T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
13.	T.TRANSMIT	TSF data may be disclosed or modified by an attacker while being transmitted between the TOE and its users.

3.3 Organizational Security Policies

Table 3-4 Organizational Security Policies

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

Item	Organization Security Policy	Organization Security Policy Description
1.	P.DETECT	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.
2.	P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to Defense Perspective data and appropriate response actions taken.
3.	P.MANAGE	The TOE shall only be managed by authorized users.
4.	P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
5.	P.ACCACT	Users of the TOE shall be accountable for their actions when configuring and initiating blocks within the IDS.

6.	P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
7.	P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

4 Security Objectives

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

4.1 Security Objectives for the TOE

The security objectives for the TOE are as follows:

Table 4-1 Security Objectives for TOE

Item	TOE Objective	TOE Objective Description
1.	O.PARTPROTCT	The TOE when invoked by the underlying host OS must protect itself from unauthorized modifications and access to its functions and data within the TOE, through its own interfaces.
2.	O.IDBLOCK	The TOE must block network security threats or out-of-policy applications.
3.	O.IDSCAN	The TOE must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.
4.	O.IDSENS	The TOE 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.
5.	O.IDANLZ	The TOE must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
6.	O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
7.	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
8.	O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
9.	O.OFLOWS	The TOE must appropriately handle potential audit and defense perspective data storage overflows, through its own interfaces.
10.	O.AUDITS	The TOE must record audit records for accesses and use of the System blocking function.
11.	O.PARTINTEGR	The TOE with the support of the underlying host OS must ensure the integrity of all audit and defense perspective data, through its own interfaces.

4.2 Security Objectives for the Environment

The TOEs operating environment must satisfy the following objectives. Most of these objectives do not levy any IT requirements but are satisfied by procedural or administrative measures.

4.2.1 Security Objectives for the IT Environment

The security objectives for the IT environment are as follows:

Table 4-2 Security Objectives for the IT Environment

Item	IT Environment Objective	IT Environment Objective Description
12.	OE.COLLECTEVENTVULN	The IT Environment must collect event and vulnerability data of an IT System.
13.	OE.OFLOWS	The IT Environment must appropriately handle potential audit and defense perspective data storage overflows, through the IT Environment's interfaces

Item	IT Environment Objective	IT Environment Objective Description
14.	OE.PARTINTEGR	The IT Environment must ensure the integrity of all audit and defense perspective data, through the IT Environment's interfaces within its scope of control.
15.	OE.PARTPROTCT	The IT Environment must protect itself from unauthorized modifications and access to its functions and data within the TOE, through the IT Environment's interfaces within its scope of control**.**
16.	OE.PROTCTCOMM	The IT environment must protect communications between the TOE and its components.
17.	OE.TIME	The underlying operating system will provide reliable time stamps.

Table 4-3 Security Objectives for the Non-IT Environment

Item	Non-IT Environment Objective	Non-IT Environment Description Objective
18.	ON.INSTALL	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.
19.	ON.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
20.	ON.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
21.	ON.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
22.	ON.INTROP	The TOE is interoperable with the IT System it monitors.
23.	ON.EXPORT	When any IDS component makes its data available to other IDS components, the IT Environment will ensure the confidentiality of the defense perspective data.
24.	ON.PASSWD	Personnel working as authorized users must follow the password policy parameters in the TOE guidance about choosing good passwords such as minimum length requirements.
25.	ON.PRTCTCOMM	Those responsible for the TOE will ensure the communications between the TOE components are secure via a SSL secure channel.

5 IT Security Requirements

This section provides the TOE security functional and assurance requirements. In addition, the IT environment security functional requirements on which the TOE relies are described. Formatting Conventions

The notation, formatting, and conventions used in this security target (ST) are consistent with version 2.3 of the Common Criteria for Information Technology Security Evaluation. Font style and clarifying information conventions were developed to aid the reader.

The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined in Common Criteria, Part 2 and paragraph 2.1.4 as:

- assignment: allows the specification of an identified parameter;
- refinement: allows the addition of details or the narrowing of requirements;
- selection: allows the specification of one or more elements from a list; and
- iteration: allows a component to be used more than once with varying operations.

This ST indicates which text is affected by each of these operations in the following manner:

- *Assignments* and *Selections* specified by the ST author are in **[*italicized bold text*]**.
- *Refinements* are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in ***italicized bold and underlined text***.
- *Iterations* are identified with a dash number "-#". These follow the short family name and allow components to be used more than once with varying operations. "*" refers to all iterations of a component.
- *Explicitly stated requirements* are named "_EXP" to denote that the requirement has been explicitly stated. For example IDS_ANL_EXP.1.
- *Application notes* provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text.*
- *Comments* are provided as an aid to the ST author and evaluation team. These items will be deleted in the final version of the ST.

5.1 TOE Security Functional Requirements

The functional security requirements for the TOE consist of the following components derived from Part 2 of the CC and explicit components, summarized in the Table 5-1 below.

Table 5-1 Functional Components

No.	Component	Component Name
1.	FAU_LOG_EXP.1	Audit log generation
2.	FAU_GEN.2	User identity association
3.	FAU_SAR.1	Audit review
4.	FAU_SAR.2	Restricted audit review
5.	FIA_ATD.1*	User attribute definition
6.	FIA_SOS.1	Verification of secrets
7.	FIA_UAU.2	User authentication before any action
8.	FIA_UID.2	User identification before any action

No.	Component	Component Name
9.	FMT_MTD.1*	Management of TSF data
10.	FMT_SMF.1	Specification of management functions
11.	FMT_SMR.1	Security roles
12.	FPT_RVM_EXP.1-1	Non-bypassability of the TSP
13.	IDS_DPD_EXP.1	Defense perspective data collection
14.	IDS_ANL_EXP.1	Analyzer analysis
15.	IDS_SA_EXP.1	Security alarms
16.	IDS_SR_EXP.1	Security response
17.	IDS_RDR_EXP.1	Restricted data review
18.	IDS_STG_EXP.1-1	Guarantee of defense perspective data availability
19.	IDS_DRS_EXP.1	Data reporting

5.1.1 Class FAU: Security Audit

FAU_LOG_EXP.1 Audit log generation

Hierarchical to: No other components.

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

a) All auditable events for the **[*not specified*]** level of audit; and

b) **[*the following auditable events:***

- ***QRadar Response Module (Offence Resolution) Audit:***
  - ***Blocks generated by the TOE, both automatically based on the alert rules and by an authorized User;***
  - ***the addition, modification, and deletion of the configuration information that specifies the blocks.***

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST: **[*no additional audit information*]**.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.2 User identity association

Hierarchical to: No other components.

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide **[*Administrator and Users with Offence Resolution privileges*]** with the capability to read **[*all audit information and audit information for the User, respectively*]** 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

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

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

Dependencies: FAU_SAR.1 Audit review

5.1.2 Class FIA: Identification and Authentication

FIA_ATD.1-1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1-1 **Refinement:** The TSF shall maintain the following list of security attributes belonging to ***administrators and Customer Support*** users:

- **[*User Name ;***
- ***Authentication data ;***
- ***Assigned Role, either Administrator or Customer Support.*]**

Dependencies: No dependencies.

Application note: The access privileges held by a user acting in the Customer Support Role is defined in **FMT_MTD.1-4***, while the privileges held by a user acting in the Administrator Role are defined in* **FMT_MTD.1-1***.*

FIA_ATD.1-2 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1-2 **Refinement:** The TSF shall maintain the following list of security attributes belonging to ***users***:

- **[*User Name;***
- ***Authentication data;***
- ***CIDR Address Ranges;***
- ***Assigned Privileges (Reports, Offence Resolution, Offense Manager, Network Surveillance)*]**

Dependencies: No dependencies.

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **[*a length greater than or equal to 5, and may contain numeric, underscore, hyphen, lower case and upper case characters*].**

Dependencies: No dependencies

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

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

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

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.

5.1.3 Class FMT: Security Management (FMT)

FMT_MTD.1-1 Management of TSF data

Application Note: FMT_MTD.1-1 describes the management of TSF data in regards to the Administration of Security Functions

FMT_MTD.1.1-1 The TSF shall restrict the ability to **[*Operations listed below*]** the **[*TSF data listed below*]** to **[*Administrator*]:**

Table 5-2 Administrator Management of TSF data

Operations selection and assignment	TSF Data Assignment
query, modify, delete	Security Management Data: • TSF data required to manage users Identification and Authentication, see the attributes defined in FIA_ATD.1* except 'password'. IDS Data: • Configure collection of data from IDS_DPD_EXP.1. • Configure and initiate 'blocks' based on all the Defense Perspective Data. • Configure the Global Exclusions, the addresses protected from blocks. • Reporting interface to all the Defense Perspective Data • Rules and Sentries applied to Offense Manager data and flow data, respectively, from which alerts (IDS_SA_EXP.1) and blocks (IDS_SR_EXP.1) are generated, includes email notification and logging. • Threshold level and email notice location for Defense Perspective data storage required for IDS_STG_EXP.1-1. • Define the data to be collected by the QFlow Collectors, as specified in IDS_DPD_EXP.1,
Query	Security Management Data: • Audit log data IDS Data: • All Defense Perspective Data • Alerts generated by the TSF • Blocks generated by the TSF

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1-2 Management of TSF data

Application Note: FMT_MTD.1-2 describes the management of TSF data in regards to the Users with Privileges.

FMT_MTD.1.1-2 **Refinement:** The TSF shall restrict the ability to **[*Operations listed below*]** the **[*TSF data listed below for the data related to the CIDR ranges specified by the Administrator for each User*]** to **[*Role Assignment listed below*].**

Table 5-3 Users Management of TSF data

Operations selection and assignment	TSF Data Assignment	Role Assignment
Query	Pre-defined Dashboard Report	Users
Query, modify, delete, create	Configure and initiate 'blocks' based on the Defense Perspective Data	Users ***with Offence Resolution privileges***
Query	Blocks generated by the TSF	
Query	Audit log data	
Query, modify, delete, create	Reporting interface to the Defense Perspective Data	Users ***with Reports privileges***
Query, modify, delete, create	Configuration for rules applied to the Offense Manager data from which Alerts (IDS_SA_EXP.1) and blocks (IDS_SR_EXP.1) are generated, includes email notification and logging.	Users ***with Offense Manager with Customized Rule privileges***
Query, modify, delete, create	Configuration for the Sentries applied to the flow data from which alerts (IDS_SA_EXP.1) and blocks (IDS_SR_EXP.1) are generated, includes email notification and logging.	Users ***with Network Surveillance and*** Users ***with Offense Manager privileges***
Query	Flow data	
Query	Rules and Sentries applied to Offense Manager data and flow data, respectively, from which alerts (IDS_SA_EXP.1) and blocks (IDS_SR_EXP.1) are generated	Users ***with Offense Manager privileges***

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1-3 Management of TSF data

Application Note: FMT_MTD.1-3 describes the management of TSF data in regards to Users with sharing privileges.

FMT_MTD.1.1-3 **Refinement:** The TSF shall restrict the ability to **[*query*]** the **[**

- ***Reporting interface to the Defense Perspective Data for User-specified CIDR ranges within the (granting) Users domain, and***
- ***Alerts on Defense Perspective Data for User-specified CIDR ranges within the (granting) Users domain*]**
  to **[*Users*] *with User-specified report sharing privileges and Offense Manager sharing privileges, respectively.***

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1-4 Management of TSF data

Application Note: FMT_MTD.1-4 describes the management of TSF data in regards to Customer Support Users.

FMT_MTD.1.1-4 The TSF shall restrict the ability to **[*query*]** the **[*'blocks' based on the Defense Perspective Data*]** to **[*Customer Support*].**

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1-5 Management of TSF data

Application Note: FMT_MTD.1-5 describes the management of TSF data in regards to the management of passwords.

FMT_MTD.1.1-5 The TSF shall restrict the ability to **[*see table below*]** the **[*see table below*]**

to **[*see table below*].**

Table 5-4 Management of Passwords

Operations selection and assignment	TSF Data Assignment	Role Assignment
modify, delete, create	All passwords	Administrator
modify	Own password	User

Application Note: User passwords in their original state must be created by the Administrator, Customer Support Users do not manage their own passwords, they are created and maintained by the Administrator.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

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: **[*Security Management: Audit (as described in Sections 6.1.2 and 6.1.6) and I&A(as described in Sections 6.1.3);*

IDS Management: Access Control over Defense Perspective data, control over reports, blocks and alerts, as specified in FMT_MTD.1*].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles **[*Administrator, Customer Support, and User*].**

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

Dependencies: FIA_UID.1 Timing of identification

5.1.4 Class FPT: Protection of the TOE Security Functions

FPT_RVM_EXP.1-1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM_EXP.1.1-1 The TSF, when invoked by the underlying host OS, shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies.

5.1.5 IDS Component Requirements (IDS)

IDS_DPD_EXP.1 Defense perspective data collection

Hierarchical to: No other components

IDS_DPD_EXP.1.1 The TOE shall be able to collect the following information from the targeted IT System resource(s): see column 1 of Table 5-5.

IDS_DPD_EXP.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 (success or failure) of the event; and

b) The additional information specified in the Details column of Table 5-5 defense perspective data.

Table 5-5 Defense perspective data

Events	Details
Network traffic	Protocol, Application, Content, Source Port, Destination Port, source address, destination address, TCP Flags
Host Profiles	Open Ports, Services, IP address

Dependencies: No dependencies.

IDS_ANL_EXP.1 Analyzer analysis

Hierarchical to: No other components

IDS_ANL_EXP.1.1 The TOE shall perform the following analysis function(s) on all defense perspective data received:

a) behavioral and event correlation

b) No other analytical functions.

IDS_ANL_EXP.1.2 The TOE 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) Analysis results.

Dependencies: IDS_DPD_EXP.1 Defense perspective data collection

IDS_EVD_EXP.1 Event and vulnerability data collection

FPT_STM.1 Reliable time stamps

IDS_SA_EXP.1 Security alarms

Hierarchical to: No other components.

IDS_SA_EXP.1.1 The TSF shall take action to send an alert to the Offense Manager console, send the alert to the QRadar system log, or send a notification via e-mail upon detection of a potential security violation.

Dependencies: IDS_ANL_EXP.1 Analyzer analysis

IDS_SR_EXP.1 Security response

Hierarchical to: No other components

IDS_SR_EXP.1.1 The TSF shall take the following actions:

Block - Prevent network traffic from moving through the network. The QRadar Response Module (Offence Resolution) provides several blocking mechanisms.

- TCP Resets: TCP Resets have the capability to block an individual host and layer 4 sessions.
- ARP Redirection: ARP Redirection (Poisoning) blocks the host from any and all communications to other subnets/CIDRs and VLANs. ARP Redirector can redirect the quarantined host to a customizable website that informs the host that they have been quarantined.
- Network Devices: The QRadar Response Module can issue commands to 3rd party devices which support ACLs and blocking rules (such as switches, routers, and firewalls)

Application Note: The block can be enabled manually or automatically.

Dependencies: IDS_ANL_EXP.1 Analyzer analysis

IDS_RDR_EXP.1 Restricted data review

Hierarchical to: No other components

IDS_RDR_EXP.1.1 The TOE shall provide the Administrator with the capability to read all data from the Defense Perspective data.

IDS_RDR_EXP.1.2 The TOE shall provide the TOE data in a manner suitable for the user to interpret the information.

IDS_RDR_EXP.1.3 The TOE shall prohibit all users read access to the Defense Perspective data, except those users that have been granted explicit read-access.

Dependencies: IDS_DPD_EXP.1 Defense perspective data collection

IDS_EVD_EXP.1 Event data collection

IDS_STG_EXP.1-1 Guarantee of defense perspective data availability

Hierarchical to: No other components

IDS_STG_EXP.1.1-1 The TOE shall protect the stored Defense Perspective data from unauthorized deletion through its own TSFI.

IDS_STG_EXP.1.2-1 The TOE shall protect the stored Defense Perspective data from modification through its own TSFI.

IDS_STG_EXP.1.3-1 The TOE shall ensure that the most recent, limited by available storage space defense perspective data will be maintained when defense perspective data storage exhaustion occurs.

IDS_STG_EXP.1.4-1 The TOE shall send an alarm if the storage capacity has been reached.

Dependencies: IDS_DPD_EXP.1 Defense perspective data collection

IDS_EVD_EXP.1 Event data collection

IDS_DRS_EXP.1 Data Reporting

Hierarchical to: No other components

IDS_DRS_EXP.1.1 The TSF shall be able to report collected Defense Perspective data using automatically generated reports.

IDS_DRS_EXP.1.2 The TSF shall be capable of generating user defined reports.

IDS_DRS_EXP.1.3 The TSF shall be capable of generating scheduled and real-time views:

Dependencies: IDS_DPD_EXP.1 Defense perspective data collection

IDS_EVD_EXP.1 Event data collection

5.1.6 Strength of Function

The threat level for the TOE authentication function is assumed to be SOF-basic. The strength of cryptographic algorithms is outside the scope of the CC. Strength of function applies only to non-cryptographic, probabilistic or permutational mechanisms. The SOF requirement applies to the identification and authentication functionality within the TOE.

5.2 Security requirements for the IT Environment

QRadar requires that the operating system platform provide reliable time stamps. QRadar requires that the operating system provides TSF domain separation and non-bypassability. All cryptographic functions are part of the IT environment, not part of the TOE.

Table 5-6 Functional Components for the IT environment

No.	Component	Component Name
20.	FAU_STG_EXP.2	Guarantees of audit data availability
21.	FPT_RVM_EXP.1-2	Non-bypassability of the TSP
22.	FPT_SEP_EXP.1	TSF domain separation
23.	FPT_STM.1	Reliable time stamps
24.	FTP_ITC.1	Trusted path/channels
25.	IDS_STG_EXP.1-2	Prevention of Defense Perspective data loss
26.	IDS_EVD_EXP.1	Event and vulnerability data collection

5.2.1 Class FAU: Security Audit

FAU_STG_EXP.2 Guarantees of audit data availability

Hierarchical to: FAU_STG.1

FAU_STG_EXP.2.1 The IT Environment shall protect the stored TSF audit records from unauthorised deletion initiated through the IT Environment's Interfaces.

FAU_STG_EXP.2.2 The IT Environment shall be able to prevent unauthorized modifications to the TSF audit records in the audit trail initiated through the IT Environment's Interfaces.

FAU_STG_EXP.2.3 The IT Environment shall ensure that the most recent limited by available storage space audit records will be maintained when the following conditions occur: audit storage exhaustion.

Dependencies: FAU_GEN.1 Audit data generation

5.2.2 Class FPT: Protection of the TOE Security Functions

FPT_RVM_EXP.1-2 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM_EXP.1.1-2 The IT environment shall ensure that the Operating System Security Policy enforcement functions are invoked and succeed before each function within the Operating System's Scope of Control is allowed to proceed.

Dependencies: No dependencies.

FPT_SEP_EXP.1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP_EXP1.1 The IT environment shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects initiating actions through the Operating System's Interface.

FPT_SEP_EXP.1.2 The IT environment shall enforce separation between the security domains of subjects in the Operating System's Scope of Control.

Dependencies: No dependencies

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1 **Refinement:** The ***IT environment*** shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies

5.2.3 Class FTP: Trusted path/channels

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

FTP_ITC.1.1 **Refinement:** The ***IT environment*** shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 **Refinement:** The ***IT environment*** shall permit [***the TSF, or the remote trusted IT product***] to initiate communication via the trusted channel.

FTP_ITC.1.3 **Refinement:** The ***IT environment*** shall initiate communication via the trusted channel

for [***all data communication among the distributed TOE component***].

Dependencies: No dependencies

5.2.4 IDS Component Requirements (IDS)

IDS_STG_EXP.1-2 Guarantee of defense perspective data availability

Hierarchical to: No other components

IDS_STG_EXP.1.1-2 The IT environment shall protect the stored Defense Perspective data from unauthorized deletion through its own TSFI.

IDS_ STG_EXP.1.2-2 The IT environment shall protect the stored Defense Perspective data from modification through its own TSFI.

IDS_ STG_EXP.1.3-2 The IT environment shall ensure that the most recent, limited by available storage space defense perspective data will be maintained when Defense Perspective data storage exhaustion occurs.

Dependencies: No dependencies.

IDS_EVD_EXP.1 Event and vulnerability data collection

Hierarchical to: No other components

IDS_EVD_EXP.1.1 The IT environment shall be able to collect the following information from the targeted IT System resource(s): event data from network devices that produce Netflow, Jflow, and Sflow events, and vulnerability data.

Dependencies: No dependencies.

5.3 TOE Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 2 (EAL2) taken from Part 3 of the Common Criteria. None of the assurance components are refined. The assurance components are listed in Table 5-7.

Table 5-7 EAL2 Assurance Components

Item	Component	Component Title
1	ACM_CAP.2	Configuration items
2	ADO_DEL.1	Delivery procedures
3	ADO_IGS.1	Installation, generation, and start-up procedures
4	ADV_FSP.1	Informal functional specification
5	ADV_HLD.1	Descriptive high-level design
6	ADV_RCR.1	Informal correspondence demonstration
7	AGD_ADM.1	Administrator guidance
8	AGD_USR.1	User guidance
9	ATE_COV.1	Evidence of coverage
10	ATE_FUN.1	Functional testing
11	ATE_IND.2	Independent testing – sample
12	AVA_SOF.1	Strength of TOE security function evaluation
13	AVA_VLA.1	Developer vulnerability analysis

Further information on these assurance components can be found in the Common Criteria for Information Technology Security Evaluation (CCITSE) Part 3.

6 TOE Summary Specification

6.1 IT Security Functions

6.1.1 Overview

Table 6-1 Security Functional Requirements mapped to Security Functions

No.	SFRs	Security Class	Security Functions	Sub-functions
1	FAU_LOG_EXP.1	Security audit	Security Audit	AU-1
2	FAU_GEN.2	Security audit	Security Audit	AU-2
3	FAU_SAR.1	Security audit	Security Audit	AU-3
4	FAU_SAR.2	Security audit	Security Audit	AU-4
5a	FIA_ATD.1-1	Identification and authentication	Identification and Authentication	IA-1
5b	FIA_ATD.1-2	Identification and authentication	Identification and Authentication	IA-2
6	FIA_SOS.1	Identification and authentication	Identification and Authentication	IA-3
7	FIA_UAU.2	Identification and authentication	Identification and Authentication	IA-3
8	FIA_UID.2	Identification and authentication	Identification and Authentication	IA-4
9	FMT_MTD.1-1	Security management	Security Management	SM-1
10a	FMT_MTD.1-2	Security management	Security Management	SM-2
10b	FMT_MTD.1-3	Security management	Security Management	SM-3
10c	FMT_MTD.1-4	Security management	Security Management	SM-4
10d	FMT_MTD.1-5	Security management	Security Management	SM-5
10e	FMT_SMF.1	Security management	Security Management	SM-6
11	FMT_SMR.1	Security management	Security Management	SM-7
12	FPT_RVM_EXP.1-1	Protection of the TSF	Partial TSF Self-Protection	SP-1
13	IDS_DPD_EXP.1	Intrusion Detection	Intrusion Detection System	IDS-1
14	IDS_ANL_EXP.1	Intrusion Detection	Intrusion Detection System	IDS-2
15	IDS_SA_EXP.1	Intrusion Detection	Intrusion Detection System	IDS-3
16	IDS_SR_EXP.1	Intrusion Detection	Intrusion Detection System	IDS-4
17	IDS_RDR_EXP.1	Intrusion Detection	Intrusion Detection System	IDS-5
18	IDS_STG_EXP.1-1	Intrusion Detection	Intrusion Detection System	IDS-6
19	IDS_DRS_EXP.1	Intrusion Detection	Intrusion Detection System	IDS-7

6.1.2 Security Audit

6.1.2.1 AU-1 Audit trail (FAU_LOG_EXP.1)

QRadar provides an audit trail function. Audit trails are maintained by QRadar and track the actions taken by QRadar users and automated actions taken by the system.

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

- Blocks generated by the TOE, both automatically based on the alert rules and by an authorized User;

- Addition, modification, and deletion of the configuration information that specifies the blocks.

Audit Trail data is generated by the QRadar Engine and is stored in the Postgres database on the QRadar Engine server. The Offence Resolution view provides reports of Resolver and Resolver Actions (i.e.: Blocks and commands issued to layer 2 thru 4 devices). The configuration activity for the blocks is recorded in the audit log for the Resolver, and the action of the TSF generating the block is recorded in the Resolver Actions audit log.

Since the audit function is always enabled, the auditing of system startup and shutdown also indicates the startup and shutdown of the audit function.

The host platform in the IT Environment provides the timestamp for the audit records.

6.1.2.2 AU-2 User identity association (FAU_GEN.2)

QRadar is able to associate each auditable event with the identity of the TOE user that caused the event. Users activating auditable events can be identified via their username.

6.1.2.3 AU-3 Audit review (FAU_SAR.1)

QRadar provides the Administrator with the capability to read all audit information from the audit records. Users with Offence Resolution privilege can only view the audit records for resolver actions that they have created. Only the Administrator may view records created by other users.

The audit records are viewable through QRadar Console Offence Resolution view in a manner suitable for the user to interpret the information. Specifically, a search function supports the selective population of views of the audit trail. In the populated view, the audit records are presented in a tabular format and can be sorted into ascending or descending order by clicking on the column headings.

6.1.2.4 AU-4 Restricted audit review (FAU_SAR.2)

QRadar prohibits all users read access to the audit records, except those users that have been granted explicit read-access. The Administrator has implicit query access, and the Administrator grants a User the Offence Resolution privilege. Once the User has been granted the Offence Resolution privilege, the internal database will permit the user to access the audit records. The QRadar GUI is engineered so that the user's can only view the data for which they have privilege.

6.1.3 Identification and Authentication

6.1.3.1 IA-1 User attribute definition (FIA_ATD.1-1)

Consistent with FMT_MTD.1-4, Customer Support users are not assigned individual permissions, as users are, but derive their privilege from their assigned role. Their access privilege is limited to searching the current actions for blocked IPs.

The privileges held by a user acting in the Administrator Role are defined in FMT_MTD.1-1.

The TSF maintains the following user attributes for Administrators and Customer Support users:

- User Name – explicit (maintained as Unique ID);
- Authentication data – explicit (maintained as password)
- Assigned Role – explicit (defined attribute).

The role that may be assigned is either Administrators or Customer Support. If a user is not assigned a role, their access permissions are assigned individually, as required by FIA_ATD.1-2.

6.1.3.2 IA-2 User attribute definition (FIA_ATD.1-2)

Operationally, the Administrator may assign privileges directly to users, or create a customized user role, assign permissions to that role, and then assign that role to users. The TSF maintains the following attributes for users:

- User Name – explicit (maintained as Unique ID);,
- Authentication data – explicit (maintained as password),
- CIDR Address Ranges – explicit (defined attribute);
- Assigned Privileges (Reports, Offence Resolution, Offence Manager, Network Surveillance) – explicit (defined attribute)

Within the Offense Manager privilege, a user can be granted additional access to customized rule creation functionality, viewing vulnerability assessment data, and performing vulnerability assessment scans. Within the Network Surveillance privilege, a user can be granted additional access to content captured using the data mine function and the data mine content. Within the Reporting functionality privilege, a user can be granted additional access to distribute reports via email and maintain report templates.

6.1.3.3 IA-3 User authentication (FIA_UAU.2 and FIA_SOS.1)

QRadar provides a password authentication mechanism to authenticate users before they are able to access the TOE.

The required password length is greater than 4 characters. The character set available for passwords included upper and lower case alphanumeric characters and special characters. Users are trained to pick passwords that include upper and lower case characters as well as at least one numeric and special character.

The password is encrypted prior to storage using a modified implementation of the MD5 hash.

6.1.3.4 IA-4 User identification (FIA_UID.2)

QRadar identifies users before they are able to access the TOE. Users are identified by their supplied user name.

6.1.4 Security Management

6.1.4.1 SM-1 Management of TSF Data (FMT_MTD.1-1)

FMT_MTD.1-1 describes operations that a user assigned to the Administrator role may perform on the specified TSF data (See Table 5-2 in Section 5.1).

6.1.4.2 SM-2 Management of TSF Data (FMT_MTD.1-2)

FMT_MTD.1-2 describes the management of TSF data with respect to granting User permissions on the basis of the source and destination IP address recorded in the collected data. QRadar is able to restrict the ability to query the Defense Perspective Data for the IP address range specified by the Administrator for each User. It also describes the management of TSF data in regards to specific privileges (See Table 5-3 in Section 5.1).

6.1.4.3 SM-3 Management of TSF Data (FMT_MTD.1-3)

FMT_MTD.1-3 describes the management of TSF data with respect to User data sharing privileges. Users with User-specified report sharing privileges and Offence Manager sharing privileges, respectively are able to query the:

- Reporting interface to the Defense Perspective Data for User-specified IP address ranges within the (granting) Users domain, and
- Alerts on Defense Perspective Data for User-specified IP address ranges within the (granting) Users domain.

A user permitted to grant access to alerts and the reports interface may not grant access to data that is not associated with their IP address range.

6.1.4.4 SM-4 Management of TSF Data (FMT_MTD.1-4)

FMT_MTD.1-4 describes the management of TSF data in regards to Users assigned to the 'Customer Support' role. QRadar restricts the ability to query 'blocks' based on the Defense Perspective Data to Users assigned to the 'Customer Support' role.

6.1.4.5 SM-5 Management of TSF Data (FMT_MTD.1-5)

FMT_MTD.1-5 describes the management of TSF data in regards to the management of passwords (See Table 5-4 in Section 5.1). Administrators have completed control over all user passwords. Administrators may create a password in the context of creating a user account. Administrators may delete a user password in the context of removing the user account. All users may change their own password.

6.1.4.6 SM-6 Specification of Management Functions (FMT_SMF.1)

QRadar is capable of performing the following security management functions:

- Security Management: Audit and I&A;
- IDS Data Management: Access Control over Defense Perspective data, control over reports, blocks and alerts, as specified in FMT_MTD.1, iterations 1 thru 5.

6.1.4.7 SM-7 Security Roles (FMT_SMR.1)

The TOE maintains three trusted roles:

- Administrator
- Customer Support
- User

The security management privileges reserved for users granted Administrator role are described in FMT_MTD.1-1. The security management privileges reserved for users granted Customer Support role are described in FMT_MTD.1-4. The permissions that define the User role capabilities are described in FMT_MTD.1-2, FMT_MTD.1-3, and FMT_MTD.1-5.

6.1.5 Partial TSF Self-Protection

6.1.5.1 SP-1 Non-bypassability (FPT_RVM_EXP.1-1)

Upon being invoked by the OS, the TSF maintains a security domain for its own execution and ensures that TOE security functions are non-bypassable. The TOE ensures that security protection and enforcement functions are invoked and succeed before each function within its scope of control is allowed to proceed.

The TOE includes three network connections that must be considered in terms of non-bypassability.

- The connection from the TOE Engine and Console component to the External User.
- The connection of the TOE Engine and Console component to the Collector
- The connection of the TOE Engine and Console component to the External Event Collector

In combination with the IT environment, the TOE environment ensures all information from an external client (e.g.: external user, Collector, External Event Collector) to the Engine and Console component or vice versa goes through the TSF. The TSF ensures that all information must flow through the policy enforcement mechanisms.

In order for an external user to access Engine and Console component, the external user must use a encrypted connection between the External user and the TSF. The encrypted connection is supported by the IT environment. The external user must provide a valid UID and authenticator (password). Once the external user is identified and authenticated, they cannot act without invoking a function or object that is protected by the TSF. Hence, the TSF ensures that all TOE security functions may only be accessed by an authorized user.

Based on the user attributes the external user's access privilege is determined for the invoked function or object. There is no communication path that passes data directly from the Collector or the External Event Collector to the External user (or vice versa) except through the TSF. Hence, the TSF ensures that all information collected from the IT environment must flow through the policy enforcement mechanisms before being accessed by an external user.

In order for a Collector or External Event Collector to access the Engine and Console component of the TOE, the connection from the Collector or External Event Collector to the Engine and Console component must be specifically configured by the Administrator. The Administrator is responsible to ensure the security of this connection, either thru physical protection, or an encrypted connection. There is no communication path that passes data directly from the Collector to the External Event Collector (or vice versa). Hence, the TSF ensures that all information collected or passed to the Collector or External Event Collector must flow through the policy enforcement mechanisms, and the Collector or External Event Collector cannot act except to pass data to the TOE server, and to accept data from the TOE server.

Further protection is provided by the underlying assumption regarding the operation of QRadar is that it is maintained in a physically secure environment.

Hence, in combination with the IT environment, the TSF ensures that all information must flow through the policy enforcement mechanisms.

6.1.6 Intrusion Detection System Functions

6.1.6.1 IDS-1 Defense perspective data collection (IDS_DPD_EXP.1)

QRadar collects data from the network via the QFlow Collectors, network components via the External Event Collector/DSM, and a vulnerability scanner, e.g., Nessus (http://www.nessus.org/) via the External Event Collector. Only the QFlow Collectors are within the TOE Boundary, the External Event Collector/DSMs are included only as a TOE interface.

The QFlow Collectors are attached to network links using a tap or span connection and, using a proprietary process, collect data passively from the network. QFlow Collectors, through their tap, are able to collect all data that passes the location, or a subset of the data as specified in IDS_DPD_EXP.1. This data is referred to as QFlow Data.

QFlow Collectors also collect Netflow, Jflow and Sflow data from routers, switches, etc. The Netflow/Jflow/Sflow data is collected by the QFlow Collector configured to

- listen on a specific port,
- for packets with designated device's IP address in the SrcIP field of the packet header, and
- with the TOE server's IP address in the DstIP field of the packet header, and
- via User DataGram Protocol (UDP) protocol.

These two data sets, the QFlow and Netflow/Jflow/Sflow, comprise the 'flow data' collected by QFlow Collectors.

QFlow Collectors are placed at key locations where surveillance is required. Once they have been deployed, QFlow Collectors require no daily management. QFlow Collectors are unique for three reasons:

- No Sampling - QFlow Collectors analyze all packets on the segment it is monitoring. Sampling can overlook data important for detecting policy issues as well as some Trojan and back-door programs. However, it is important to note that some QRadar v5.1.2 appliance models are licensed to be limited to a certain amount of flows.
- Layer 7 analysis - QRadar does not rely on static definitions of applications by port number. Instead it analyzes application protocol headers (Layer 7) to capture packets running on ports other than the ones expected (e.g. SSH back door), multiple ports (e.g. P2P) and even applications tunneled within other applications (e.g. IM).
- Content Capture - QRadar captures a configurable amount of content from the first part of each flow and stores URLs, filenames, and other applicable information. This allows in-depth analysis well after the event has passed.

See Table 5-5 for a list of defense perspective data that is collected by QFlow Collector.

QFlow Collectors send the collected flow data to the TOE server (QRadar Engine and Console component of the TOE) via a protected channel.

As defined in IDS_EVD_EXP.1, the event data and vulnerability analysis data are collected by the DSMs and the vulnerability scanners, respectively and forwarded to the TOE server by the External Event Collector.

Before forwarding the collected data to the TOE server, the External Event Collector standardizes and normalizes the collected data to include the: QID, Device Event ID, Device ID, Device Type, Source IP, Source Port, Destination IP, Destination Port, Device Event Count, Protocol, Category, Credibility, Severity, Relevance, Payload, Annotations, Start Time, and End Time.

The External Event Collector also sends the collected normalized data to the TOE server via a protected channel.

6.1.6.2 IDS-2 Analyzer analysis (IDS_ANL_EXP.1)

Behavioral Analysis:

Behavioral analysis is performed on the data collected by the Collector by the Flow Processor and Classification Engine subcomponents of the TOE. The analysis begins with normalizing the flow, removing duplications and, using a proprietary process (patent pending), bundling the flows to create superflows, optimizing further analysis. The optimized flow data is sent to the Classification Engine subcomponent of the TOE where classification analysis is performed creating tags for the data. The data is tagged based on the packet header data and content, and threat and policy configuration information based on parameters defined in Table 5-5, Defense perspective data.

A Sentry process on the Classification Engine further analyzes the tagged data, comparing the behavior represented by the data with policy and threat configuration information. It also analyzes the

new data and compares the product of this analysis with accumulated statistical data characterizing 'normal' behavior. Based on this processing, the Sentry may take a configured action, such as raising an alert, generating a 'block', or raising an internal event. An internal event is then further processed in a way similar to data collected by the External Event Collector.

Default Sentries are pre-configured that detect aggressive scanning or worm activity, detect changes in the number of hosts participating in client applications and port connections, detect denial of service attacks both to and from local hosts, detect changes in unidirectional and bi-directional flows, detect threats from top hostile networks, highly targeted ports, and sensitive applications, detect changes in traffic volume for upper-level objects such as large abnormal data transfers, detect network protocol anomaly, detect changes in the number of hosts participating in server port connections, detect slow scan response, detect remote access application on non-standard ports, and detect activity-level anomalies in non-TCP, UDP, and ICMP protocols.

The Sentries explicitly included in the TSF are:

1. Client Based DNS Activity to the Internet
2. Distributed DoS Attack (High Number of Hosts)
3. Distributed DoS Attack (Low Number of Hosts)
4. Distributed DoS Attack (Medium Number of Hosts)
5. Excessive Anomalous IMCP Flows
6. Excessive Inbound Unidirectional Flows Threshold
7. Excessive Outbound Unidirectional Flows Threshold
8. Excessive P2P Policy Threshold
9. Excessive Rejected Communication Attempts
10. Excessive SMTP Mail Sender
11. Excessive Unidirectional ICMP Detected
12. Excessive Unidirectional ICMP Responses Detected
13. Excessive Unidirectional TCP Flows
14. Excessive Unidirectional UDP or Misc Flows
15. Flow Count Behaviour Change
16. Hidden FTP Server
17. High Rate DoS Flood Attack
18. High Rate ICMP Scan
19. High Rate Scanning Activity
20. Host Count Behaviour Change
21. ICMP DoS
22. Invalid TCP Flag Usage
23. Local P2P Server Detected
24. Low Rate DoS Flood Attack
25. Low Rate ICMP Scan
26. Medium Rate DoS Flood Attack
27. Medium Rate ICMP Scan
28. Medium Rate Scanning Activity
29. Policy Excessive IM/Chat
30. Policy Excessive IRC Connections
31. Port 0 Flows Detected
32. Scanning Activity
33. SSH or Telnet Detected on Non-Standard Port
34. TCP DoS
35. Threat Traffic Packet Rate Behaviour Change
36. UDP DoS
37. VNC Access from the Internet to a Local Host
38. Potential Network Scan
39. Potential Unresponsive Service or Distributed DoS

Behavioral analysis is also supported through Event Rules and Offence Rules. A rule is a collection of tests and consequent actions. Each rule consists of tests, functions that logically combine tests, and building blocks which allow re-use of tests in multiple rules. Tests may be based on source and destination Network Properties, Event properties, IP/Port properties, Host Profile properties, Date and Time properties, Device properties and Offence properties.

Default Event Rules supported by the Event Processor module are: Login Failures across Multiple Hosts, Repeated Login Failures Single Host, Scan and Attack, Threat Exposure of Target Rapidly Increasing, Exploit and IRC Connect, Mass Mailing Host Detected, Drop Unwanted Events, Recon and Suspicious Activities, Multiple Firewall System Configuration Errors detected, Recon Detected Across Multiple Hosts, Suspicious Events Across Multiple Hosts, Multiple Local Hosts Connecting to Single Remote Site, Exploit Attempts Across Multiple Hosts, Multiple Attack Types Detected, Multiple System Errors or Failure Detected, and Push Policy Events to the Internal Event Collector subcomponent.

Offence Rules supported by the QRadar Engine component are Offence Syslog Sender, Offence EMAIL Sender.

Event Correlation:

Two types of events, the internal events from the Sentry and the external events from the external DSM, and the vulnerability analysis data are brought together in the QRadar Engine. The Offence Manager view permits users to analyze this combined data. The events are normalized and correlated with the goal of identifying the source attack actions with a profile that includes identifying the target assets and where the attacks are occurring. The vulnerability analysis data is also correlated with this information to help establish severity and to prioritize based on the target's vulnerability to the detected threat. Administrator-configured credibility ratings for events are also factored into the analysis.

These external and internal events are also correlated to data collected by the Collector to both reduce false positives and to track hosts associated with events. This is accomplished by the Magistrate Engine, which after receiving certain event types, makes a request to the QRadar Classification engine sub-component of the QRadar Engine to modify the real-time analysis information from incoming flows to identify network traffic that is significant to an event. The events that trigger this request are not Administrator or User configurable.

Analysis that trigger Alerts and Blocks:

Administrators and Users with privilege can create 'sentries' and 'rules' which the analysis processes can use to trigger alerts (IDS_SA_EXP.1) and blocks (IDS_SR_EXP.1).

The types of alerts a Sentry can generate are email, SNMP, or log based alerts. Rules may be used to generate email, SNMP, log based alerts, and actions (security responses) that block certain activities or resolve the Offence.

The sentries support the analysis to the raw flow data in the Magistrate subcomponent of the QRadar Engine, and the Offence rules support the analysis of the data resulting from the application of the sentries to the raw flow data, generating alerts when the Offence rule predicate is satisfied. The result of the application of the Offence rules is then processed by Event Rules where the alerts are weighted, i.e., prioritized based on the result of the Event Rules.

6.1.6.3 IDS-3 Security alarms (IDS_SA_EXP.1)

Internally, QRadar emits alerts from the sentry process on the Classification Engine. These alerts are sent to the QRadar Engine for display in the Offence Manager view on the Console via the internal event processor. The Administrator may also configure these alerts to be sent to a QRadar system log and send a notification to a designated email address.

As explained in IDS-2, there are two types of events, Internal Events generated by Sentries processing data gathered by Collectors, and External Events generated by the External Event Collector. This is collectively referred to as 'event information'.

The Offence Manager includes a Custom Rule Engine that allows Administrators and Users with appropriate privilege to create rules based on any combination of the event information. Offence Manager processes each event against these rules and can generate alarms. Based on the rule definition the alarms can be sent to the QRadar Console Offence Manager view, syslog, pager and/or e-mail. These alarms are prioritized based on the correlation analysis, e.g., factoring in vulnerabilities and credibility.

6.1.6.4 IDS-4 Security response (IDS_SR_EXP.1)

QRadar Offence Resolution is a QRadar product module that includes the capability of the QRadar Engine to block network security threats, as well as security management capabilities and user interface enhancements.

Authorized administrators and users of QRadar Offence Resolution have the option of taking any of the actions below either automatically via user-specification in the QRadar Engine, as described in IDS-3, or upon notification.

Based upon the equipment and location of a detected threat an authorized TOE user can perform a block action to mitigate the threat. The block action prevents threatening traffic (such as a worm) from proliferating through the network and infecting other hosts. To achieve the block action three mechanisms have been incorporated into QRadar Offence Resolution:

- TCP Resets
  QRadar utilizes the TCP Reset mechanism to block TCP communications of a host that has been identified to be a threat to the network. TCP Resets can be used to only shut down the threatening traffic, while allowing the host to continue running normal business applications.
- ARP Redirection
  ARP Redirection allows QRadar to quarantine a host to a specific VLAN/Subnet/CIDR to inhibit the spread of a threat to other areas of the network.
- Network Devices
  QRadar has the ability to issue ACL and rule commands to network devices such as switches routers and firewalls. ACL and rule commands can be used to configure switches, routers and firewalls to block specific hosts, ports and interfaces. The protocols thru which rule commands are directed to layer 2 thru 4 devices vary for different network devices, e.g., they include telnet, and SNMP.

The QRadar product's Offence Resolution module also includes a 'Global exclusions' mechanism which allows Administrators to prohibit blocks to a set of pre-defined IP-addresses.

6.1.6.5 IDS-5 Restricted Data Review (IDS_RDR_EXP.1)

QRadar provides the Administrator, or a User who has been granted the Network Surveillance Administrative privilege, with the capability to read all defense perspective data. The Administrator, when granting a user the Network Surveillance Administrative privilege, can restrict the read permission to specific CIDR ranges of the defense perspective data. QRadar prohibits all users read access to the event data, except those users that have been granted explicit read-access.

QRadar provides the defense perspective data in a manner that is readable for the user. QRadar provides two methods to view collected network traffic.

First, for users who have been assigned the Administrator role, or hold Network Surveillance privileges, QRadar supports Views. Each view represents all traffic activity on the network; however, each view displays the network activity in a specific profile.

The Local Network View has levels of depth, specific to the network hierarchy. The administrator can also create Custom Views to display the types of traffic the administrator wish to identify, monitor, and be alerted to, when specific flows appear in the network. The administrator must configure Custom Views with equations that identify the network activity and match the properties built into an equation. Global Views are pre-configured views that capture and display network activity.

Each view filters traffic based upon traffic attributes. Views can be configured with an identifiable color scheme. Each color that appears on the graph represents the activity occurring on the network. Each color is also displayed in the legend beside the graph. The administrator can point to the color on the legend to identify the traffic type.

The second method is the Reports capability. The user can design and generate detailed operational reports and executive summaries with the Reports function. Once the user creates a report, the user can view the results in multiple formats. The template wizard also allows the user to create a distribution list to e-mail reports or send a URL that enables online access for viewers. Available views (and traffic layers) options include: Bytes-which includes Bytes In and Bytes Out, Packets-which includes pin and pout, Number of Hosts-which includes hlocal and hremote, and Unique Ports-which includes plocal and premote.

6.1.6.6 IDS-6 Guarantee of Defense perspective data availability (IDS_STG_EXP.1-1)

QRadar stores the Defense Perspective data in 3 separate databases. The flow data is stored in a proprietary file-based database on the QRadar Engine server to a location specified during installation. The post-analysis event data is stored on the QRadar Engine server in a Postgres SQL database, and the raw event data, used to provide the forensic data with the alerts, is stored on the QRadar Engine server in a proprietary file-based database, referred to as Ariel.

QRadar protects the stored Defense Perspective data from unauthorized modification and deletion through the TSF interfaces. The QRadar v5.1.2 main screen GUI is engineered so that the user cannot delete or modify the Defense Perspective data. Also, the QRadar v5.1.2 databases are configured so that only the Engine and Console component of the TOE can update the records.

QRadar contains a QMonitor feature that signals when the storage capacity is nearing exhaustion. When the disk space utilization of the database server exceeds an Administrator-specified threshold an email notification is sent. The notice is re-sent at each 1% increment until the capacity is below the configured threshold level. The Administrator is responsible to configure the threshold so that there is sufficient time to delete older data before storage capacity is exhausted.

The Postgres database uses a QRadar process, Vacuumdb that serves as a reduction tool application. It enables the setting of an expiry date so that older audit database records are removed when the data's set expiry date is exceeded. The expiry date of the data and frequency of execution of *crontab* is configurable by the Administrator. The Administrator is responsible to configure and adjust the expiry data so that older data does not saturate the QRadar Engine server's storage capacity.

The TSF is dependent on the IT environment and hardware to protect the Defense perspective data storage from access via the OS interfaces.

6.1.6.7 IDS-7 Data Reporting (IDS_DRS_EXP.1)

QRadar provides two methods for users to view collected network traffic: the Views capability and the Reports capability.

The Views capability includes default views. Default Views include:

- Local Networks View — Displays traffic by network objects.
- Ports View — Displays traffic originating from identified destination ports.
- Applications View — Displays traffic originating from application layer by client connection and server connection.
- Remote Networks View — Displays user defined traffic originating from named remote networks.
- Remote Services View — Displays traffic originating from user defined network ranges or, if desired, the automatic update function provided by QRadar.
- Collector View — Displays traffic seen by each QFlow Collector.
- Protocol — Displays traffic originating from protocol usage.
- Flow types — Displays the calculated ratio of inbound to outbound traffic.

The Reports capability of QRadar includes a template wizard that enables scheduling, formatting, viewing, and notification capabilities. Reports may be scheduled for immediate generation by manual commend, or automatic generation on an hourly, daily, weekly, or monthly basis. Reports can be created so that they include detailed time series graphs, summarized graphs, derived vulnerability data, and a combination of charts. Reports are created using the Report Template Wizard and the defined objects. Defined objects include nets, apps, ports, geographic, remote nets, remote services, protocols, flow types, collector, IP Tracking, and Threats.

6.1.7 SOF Claims

The threat level for the TOE authentication function is assumed to be SOF-basic. This defines a level of authentication strength of function where analysis shows that the function provides basic protection against straightforward or intentional breach of TOE security by attackers possessing a minimum attack potential. The strength of cryptographic algorithms is outside the scope of the CC. Strength of function applies only to non-cryptographic, probabilistic or permutational mechanisms. The SOF requirement applies to the identification and authentication functionality within the TOE.

The overall strength of function requirement is SOF-Basic. The strength of function requirement applies to FIA_UAU.2. The SOF claim for FIA_UAU.2 is SOF-Basic. Strength of Function shall be demonstrated for the non-certificate based authentication mechanisms to be SOF-basic, as defined in Part 1 of the CC. Specifically, the TOE password authentication mechanism must demonstrate adequate protection against attackers possessing a low-level attack potential.

6.2 Assurance Measures

The TOE satisfies the assurance requirements for Evaluation Assurance Level (EAL) 2. The following items are provided as evaluation evidence to satisfy the EAL2 assurance requirements:

Table 6-2 Assurance Measures

Component	Evidence Requirements	How Satisfied
ACM_CAP.2	CM Documentation • CM Proof • Configuration Item List	ACM_CAP.2 - QRadar 5.1.2 file list. ACM_CAP.2 - QRadar 5.1.2 file list - history

Component	Evidence Requirements	How Satisfied
ADO_DEL.1	Delivery Procedures	Q1 Labs QRadar Reference Guide 5.1 Q1 Labs QRadar Getting Started With QRadar Appliances 5.1, May 2006 Q1 Labs QRadar Installation Guide 5.1, May 2006 QRadar Release Notes; Release 5.1.2; August 2006
ADO_IGS.1	Installation, generation, and start-up procedures	Q1 Labs QRadar Getting Started With QRadar Appliances 5.1, May 2006 QRadar Release Notes; Release 5.1.1; August 2006 QRadar Release Notes; Release 5.1.2; August 2006 Q1 Labs Q1 Labs QRadar™ 5.1 Common Criteria Supplement to the Guidance Documentation", V0.1, October 28, 2006
ADV_FSP.1	Functional Specification	Q1 Labs QRadar 5.1 EAL2 Common Criteria Evaluation Proprietary Development Specification, v 0.12, December 5, 2005
ADV_HLD.1	High-Level Design	Q1 Labs QRadar 5.1 EAL2 Common Criteria Evaluation Proprietary Development Specification, v 0.12, December 5, 2005
ADV_RCR.1	Representation Correspondence	Q1 Labs QRadar 5.1 EAL2 Common Criteria Evaluation Proprietary Development Specification, v 0.12, December 5, 2005
AGD_ADM.1	Administrator Guidance	Q1 Labs QRadar Administration Guide 5.1, July 2006 Q1 Labs QRadar Users Guide 5.1, May 2006 Q1 Labs QRadar Getting Started With QRadar Appliances 5.1, May 2006 Q1 Labs Q1 Labs™ QRadar™ 5.1 Common Criteria Supplement to the Guidance Documentation", V0.1, October 28, 2006 Offence Resolution Users Guide, Release 2.0, May 2006
AGD_USR.1	User Guidance	Not applicable for this product
ATE_COV.1	Test Coverage Analysis	Test Coverage for Q1 Labs QRadar, October 27, 2006
ATE_FUN.1	Test Documentation	Q1 Labs QRadar 5.1 EAL2 Common Criteria Evaluation Proprietary Development Specification, v 0.12, December 5, 2005 Enterprise_Sentries_Test_Plan.doc, September 7, 2006 IdenAuth#2.doc, September 7, 2006 SecureAudit#1.doc, September 7, 2006 SecurityManage#3.doc, September 7, 2006 IDS#5.doc, September 7, 2006 TSFProtect#4.doc, September 7, 2006 Common Criteria Certification Test Environment Specification, September 29, 2006 CC test Summary, Version 0.3, September 7, 2006
ATE_IND.2	TOE for Testing	TOE for Testing, QRadar Version 5.1.2 Evaluation Team Test Plan: Q1 Labs QRadar V5.1.2, Version 0.4, October 26, 2006 Evaluation Team Test Report: Q1 Labs QRadar V5.1.2, Version1.0, December 18, 2006
AVA_SOF.1	SOF Analysis	Common Criteria Security Assurance Measures – Strength of TOE Function Claims Evaluation - AVA_SOF.1, V. 1.3
AVA_VLA.1	Vulnerability Analysis	Common Criteria Security Assurance Measures – (EAL2) Developer Vulnerability Analysis – AVA_VLA.1, version 1.4, September 13, 2006

7 PP Claims

The QRadar Security Target was not written to address any existing Protection Profile.

8 Rationale

8.1 Security Objectives Rationale

8.1.1 Threats to Security

Table 8-1 shows that all the identified threats to security are countered by Security Objectives for the TOE and IT Environment. Rationale is provided for each threat below the table.

Table 8-1 All Threats to Security Countered

Item	Threat Name	Security Objective
1	T.COMINT	O.PARTPROTCT O.ACCESS O.IDAUTH O.PARTINTEGR OE.PARTPROTCT OE.PARTINTEGR OE.TIME
2	T.COMDIS	O.PARTPROTCT O.ACCESS O.IDAUTH ON.EXPORT OE.PARTPROTCT OE.PARTINTEGR OE.TIME
3	T.NOHALT	O.IDAUTH O.ACCESS O.IDSCAN O.IDSENS O.IDANLZ OE.COLLECTEVENTVULN
4	T.PRIVIL	O.PARTPROTCT O.ACCESS O.IDAUTH OE.PARTPROTCT OE.PARTINTEGR OE.TIME
5	T.IMPCON	O.EADMIN O.ACCESS O.IDAUTH ON.INSTALL
6	T.INFLUX	O.OFLOWS OE.OFLOWS
7	T.FACCNT	O.AUDITS
8	T.SCNCFG	O.IDSCAN O.IDBLOCK OE.COLLECTEVENTVULN

Item	Threat Name	Security Objective
9	T.SCNMLC	O.IDSCAN O.IDBLOCK OE.COLLECTEVENTVULN
10	T.SCNVUL	O.IDSCAN OE.COLLECTEVENTVULN
11	T.FALASC	O.IDANLZ
12	T.MISUSE	O.IDSENS
13	T.TRANSMIT	OE.PROTCTCOMM

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

- O.PARTPROTCT: The TOE when invoked by the underlying host OS must protect itself from unauthorized modifications and access to its functions and data within the TOE, through its own interfaces. This objective provides for access controls that protect the TSF data from unauthorized modifications and accesses.
- O.ACCESS: The TOE must allow authorized users to access only appropriate TOE functions and data. This objective builds upon the O.IDAUTH objective by only permitting authorized users to access TSF data.
- O.IDAUTH: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of users prior to any TSF data access.
- O.PARTINTEGR: The TOE with the support of the underlying host OS must ensure the integrity of all audit and defense perspective data, through its own interfaces. This objective provides for the integrity of all audit and defense perspective data.
- OE.PARTINTEGR: The IT Environment must ensure the integrity of all audit and defense perspective data, through the IT Environment's interfaces within its scope of control. This objective provides for the integrity of all audit and defense perspective data by the IT Environment.
- OE.PARTPROTCT: The IT Environment must protect itself from unauthorized modifications and access to its functions and data within the TOE, through the IT Environment's interfaces within its scope of control. This objective provides for the IT Environment to protect itself from unauthorized modifications and access to its functions and data within the TOE.
- OE.TIME: The underlying operating system will provide reliable time stamps. This objective provides for the IT Environment to provide reliable time stamps

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

- O.PARTPROTCT: The TOE when invoked by the underlying host OS must protect itself from unauthorized modifications and access to its functions and data within the TOE, through its own interfaces. This objective provides for access controls that protect the TSF data from unauthorized modifications and accesses.
- O.ACCESS: The TOE must allow authorized users to access only appropriate TOE functions and data. This objective builds upon the O.IDAuth objective by only permitting authorized users to access TSF data.
- O.IDAUTH: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of users prior to any TSF data access.
- ON.EXPORT: When any IDS component makes its data available to other IDS components, the IT Environment will ensure the confidentiality of the defense perspective data. This objective provides for the IT Environment to provide encryption capabilities to protect the TSF data from being disclosed.

- OE.PARTINTEGR: The IT Environment must ensure the integrity of all audit and defense perspective data, through the IT Environment's interfaces within its scope of control. This objective provides for the integrity of all audit and defense perspective data by the IT Environment.
- OE.PARTPROTCT: The IT Environment must protect itself from unauthorized modifications and access to its functions and data within the TOE, through the IT Environment's interfaces within its scope of control. This objective provides for the IT Environment to protect itself from unauthorized modifications and access to its functions and data within the TOE.
- OE.TIME: The underlying operating system will provide reliable time stamps. This objective provides for the IT Environment to provide reliable time stamps

T.NOHALT: An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE. T.NOHALT is countered by:

- O.IDAUTH: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of users prior to any TSF data access
- O.ACCESS: The TOE must allow authorized users to access only appropriate TOE functions and data. This objective builds upon the O.IDAUTH objective by only permitting authorized users to access TSF data.
- O.IDSCAN: The TOE must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System. This objective ensures the TOE collects and stores static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System. This includes attempts at halting the TOE.
- O.IDSENS: The TOE 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. This objective ensures the TOE collects and stores information about all events including attempts at halting the TOE.
- O.IDANLZ: The TOE must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future). This objective ensures that the TOE must apply analysis to the event data gathered by the TOE. This includes attempts at halting the TOE.
- OE.COLLECTEVENTVULN: The IT Environment must collect event and vulnerability data of an IT System. This objective ensures that the IT Environment collect event and vulnerability data that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System. This includes attempts at halting the TOE.

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

- O.PARTPROTCT: The IT Environment must protect itself from unauthorized modifications and access to its functions and data within the TOE, through the IT Environment's interfaces within its scope of control. This objective provides for access controls that protect the TSF data from unauthorized modifications and accesses.
- O.ACCESS: The TOE must allow authorized users to access only appropriate TOE functions and data. This objective builds upon the O.IDAUTH objective by only permitting authorized users to access TSF data.
- O.IDAUTH: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of users prior to any TSF data access.
- OE.PARTINTEGR: The IT Environment must ensure the integrity of all audit and defense perspective data, through the IT Environment's interfaces within its scope of control. This objective provides for the integrity of all audit and defense perspective data by the IT Environment.

- OE.PARTPROTCT: The IT Environment must protect itself from unauthorized modifications and access to its functions and data within the TOE, through the IT Environment's interfaces within its scope of control. This objective provides for the IT Environment to protect itself from unauthorized modifications and access to its functions and data within the TOE.
- OE.TIME: The underlying operating system will provide reliable time stamps. This objective provides for the IT Environment to provide reliable time stamps

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

- O.EADMIN: The TOE must include a set of functions that allow effective management of its functions and data. This objective ensures the TOE has all the necessary administrator functions to manage the product.
- O.ACCESS: The TOE must allow authorized users to access only appropriate TOE functions and data. This objective builds upon the O.IDAUTH objective by only permitting authorized users to access TSF data.
- O.IDAUTH: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of users prior to any TSF data access.
- ON.INSTALL: 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. This objective provides for the secure installation and operation of the TOE.

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

- O.OFLOWS: The TOE must appropriately handle potential audit and defense perspective data storage overflows, through its own interfaces This objective counters this threat by requiring the TOE handle data storage overflows.
- OE.OFLOWS: The IT Environment must appropriately handle potential audit and defense perspective data storage overflows, through the IT Environment's interfaces This objective counters this threat by requiring the IT Environment to handle data storage overflows.

T.FACCNT: Unauthorized attempts to access TOE data or security functions may go undetected. T.FACCNT is countered by:

- O.AUDITS: The TOE must record audit records for accesses and use of the System blocking function. This objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.

T.SCNCFG: Improper security configuration settings may exist in the IT System the TOE monitors. T.SCNCFG is countered by:

- O.IDSCAN: The TOE must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System. This objective provides for the TOE collecting and storing static configuration information that may be indicative of a configuration settings change.
- O.IDBLOCK: The TOE must block network security threats or out-of-policy applications. This objective provides for the TOE taking corrective actions to configure the network appliances and IT Systems the TOE monitors to isolate network security threats.
- OE.COLLECTEVENTVULN: The IT Environment must collect event and vulnerability data of an IT System. This objective ensures that the IT Environment collects event and vulnerability data that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.

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

- O.IDSCAN: The TOE must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System. This objective provides for the TOE collecting and storing static configuration information from the IT Systems the TOE monitors. Static configuration information may be indicative of, or may be modified so as to indicate, the past action or presence of malicious code.
- O.IDBLOCK: The TOE must block network security threats or out-of-policy applications. The TOE isolates out-of-policy applications thru taking corrective actions to configure the network appliances and IT Systems the TOE monitors. These corrective actions could prevent the execution of, or mitigate the effects of executing malicious code.
- OE.COLLECTEVENTVULN: The IT Environment must collect event and vulnerability data of an IT System. This objective ensures that the IT Environment collect event and vulnerability data that might be indicative of malicious code being present on IT Systems the TOE monitors.

T.SCNVUL: Vulnerabilities may exist in the IT System the TOE monitors. T.SCNVUL is countered by:

- O.IDSCAN: The TOE must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System. This objective provides for the TOE collecting and storing static configuration information from the IT Systems the TOE monitors. Static configuration information may be indicative of vulnerabilities on the IT systems the TOE monitors.
- OE.COLLECTEVENTVULN: The IT Environment must collect event and vulnerability data of an IT System. This objective ensures that the IT Environment collect event and vulnerability data that might be indicative of the potential for a vulnerability that exists in the IT Systems the TOE monitors.

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

- O.IDANLZ: The TOE must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future). This objective provides the function that the TOE will identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

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

- O.IDSENS: The TOE 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. This objective ensures the TOE collects and stores information about all events including attempts at misuse.

T.TRANSMIT: TSF data may be disclosed or modified by an attacker while being transmitted between the TOE and its users.

- OE.PROTCTCOMM: The IT environment must protect communications between the TOE and its components. This objective ensures the IT environment will protect communications between the TOE and its components.

8.1.2 Organizational Security Policies

Table 8-2 shows that all the identified organizational security policies are covered by Security Objectives for the TOE and IT Environment. Rationale is provided for each organizational security policy below the table.

Table 8-2 All Organizational Security Policies are addressed

Item	Organizational Security Policy	Security Objective
1	P.DETECT	O.AUDITS O.IDSENS O.IDSCAN OE.COLLECTEVENTVULN
2	P.ANALYZ	O.IDANLZ, O.IDBLOCK
3	P.MANAGE	ON.PERSON O.EADMIN ON.INSTALL O.IDAUTH O.ACCESS ON.CREDEN O.PARTPROTCT
4	P.ACCESS	O.IDAUTH O.ACCESS O.PARTPROTCT
5	P.ACCACT	O.AUDITS O.IDAUTH
6	P.INTGTY	O.PARTINTEGR
7	P.PROTCT	O.OFLOWS ON.PHYCAL OE.OFLOWS

P.DETECT: Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected. P.DETECT is covered by:

- O.AUDITS: The TOE must record audit records for accesses and use of the System blocking function. This objective ensures the TOE will audit attempts for data accesses and use of TOE functions.
- O.IDSENS: The TOE 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. This objective ensures the TOE collects and stores information about all events.
- O.IDSCAN: The TOE must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System. This objective ensures the TOE collects and stores static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.
- OE.COLLECTEVENTVULN: The IT Environment must collect event and vulnerability data of an IT System. This objective ensures that the IT Environment collect event and vulnerability data that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System. This includes attempts at halting the TOE.

P.ANALYZ: Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to Defense Perspective data and appropriate response actions taken. P.ANALYZ is covered by:

- O.IDANLZ: The TOE must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future). This objective requires analytical processes are applied to data collected from Sensors and Scanners.
- O.IDBLOCK: The TOE must block network security threats or out-of-policy applications. This objective requires that the TOE provide a blocking mechanism.

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

- ON.PERSON: Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System. This objective ensures that the authorized administrators will be competent and well trained.
- O.EADMIN: The TOE must include a set of functions that allow effective management of its functions and data. This objective ensures the TOE has all the necessary administrator functions to manage the product.
- ON.INSTALL: 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. This objective supports the ON.PERSON objective by ensuring administrators follow all provided documentation and maintain the security policy.
- O.IDAUTH: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for the identification and authentication of users prior to any TSF data access.
- O.ACCESS: The TOE must allow authorized users to access only appropriate TOE functions and data. This objective builds upon the O.IDAUTH objective by only permitting authorized users to access TSF data.
- ON.CREDEN: Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security. This objective requires administrators protect all authentication data.
- O.PARTPROTCT: The TOE when invoked by the underlying host OS must protect itself from unauthorized modifications and access to its functions and data within the TOE, through its own interfaces. This objective provides for access controls that protect the TSF data from unauthorized modifications and accesses. This objective provides TOE self-protection.

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

- O.IDAUTH: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for the identification and authentication of users prior to any TSF data access.
- O.ACCESS: The TOE must allow authorized users to access only appropriate TOE functions and data. This objective builds upon the O.IDAUTH objective by only permitting authorized users to access TSF data.
- O.PARTPROTCT: The TOE when invoked by the underlying host OS must protect itself from unauthorized modifications and access to its functions and data within the TOE, through its own interfaces. This objective provides for access controls that protect the TSF data from unauthorized modifications and accesses. This objective provides TOE self-protection.

P.ACCACT: Users of the TOE shall be accountable for their actions when configuring and initiating blocks within the IDS. P.ACCACT is covered by:

- O.AUDITS: The TOE must record audit records for accesses and use of the System blocking function. This objective requires the TOE to audit attempts for data accesses and use of TOE functions.
- O.IDAUTH: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for the identification and authentication of users prior to any TSF data access.

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

- O.PARTINTEGR: The TOE with the support of the underlying host OS must ensure the integrity of all audit and defense perspective data, through its own interfaces. This objective provides for the integrity of all audit and defense perspective data

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

- O.OFLOWS: The TOE must appropriately handle potential audit and defense perspective data storage overflows, through its own interfaces. This objective counters this threat by requiring the TOE handle data storage overflows.
- ON.PHYCAL: Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack. This objective provides for the physical protection of the TOE by authorized administrators.
- OE.OFLOWS: The IT Environment must appropriately handle potential audit and defense perspective data storage overflows, through the IT Environment's interfaces This objective counters this threat by requiring the IT Environment to handle data storage overflows.

8.1.3 Assumptions

Table 8-3 shows that all the identified assumptions are covered by Security Objectives for the TOE and IT Environment. Rationale is provided for each assumption below the table.

Table 8-3 All Assumptions Addressed

Item	Name	Objective
1	A.ACCESS	ON.INTROP
2	A.DYNAMIC	ON.INTROP ON.PERSON
3	A.MANAGE	ON.PERSON
4	A.NOEVIL	ON.INSTALL ON.PHYCAL ON.CREDEN
5	A.PASSWD	ON.PASSWD
6	A.PROTCT	ON.PHYCAL
7	A.PROTCTCOMM	ON.PRTCTCOMM
8	A.SCOPE	ON.INTROP
9	A.TRUSTED	ON.PHYCAL ON.CREDEN

A.ACCESS: The TOE has access to all the IT security management data and defense perspective data it needs to perform its functions. A.ACCESS is covered by:

- ON.INTROP: The TOE is interoperable with the IT System it monitors. This objective ensures the TOE has the needed access to the IT System.

A.DYNAMIC: The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors. A.DYNAMIC is covered by:

- ON.INTROP: The TOE is interoperable with the IT System it monitors. This objective ensures the TOE has the needed access to the IT System.
- ON.PERSON: Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System. This objective ensures that the TOE will be managed appropriately.

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

- ON.PERSON: Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System. This objective ensures that all authorized administrators are qualified and trained to manage the TOE.

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

- ON.INSTALL: 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. This objective ensures that the TOE is properly installed and operated.
- ON.PHYCAL: Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack. This objective provides for the physical protection of the TOE by authorized administrators.
- ON.CREDEN: Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security. This objective supports this assumption by requiring protection of all authentication data.

A.PASSWD: The TOE has access to all the IT security management data and defense perspective data it needs to perform its functions. A.PASSWD is covered by:

- ON.PASSWD: Personnel working as authorized users must follow the password policy parameters in the TOE guidance about choosing good passwords such as minimum length requirements. This objective provides for authorized administrators following the supplied guidance to create good passwords.

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

- ON.PHYCAL: Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack. This objective provides for the physical protection of the TOE hardware and software.

A.PROTCTCOMM: Those responsible for the TOE will ensure the communications between the TOE components are secure via a SSL secure

- OE.PROTCTCOMM: Those responsible for the TOE will ensure the communications between the TOE components are secure via a SSL secure channel. This objective is a restatement of the assumption. This objective ensures those responsible for the TOE will ensure the communications between the TOE components are secure via a SSL secure channel.

A.SCOPE: The TOE is appropriately scalable to the IT System the TOE monitors. A.SCOPE is covered by:

- ON.INTROP: The TOE is interoperable with the IT System it monitors. This objective ensures the TOE has the necessary interactions with the IT System it monitors.

A.TRUSTED: There will be no untrusted users of the TOE and no untrusted software loaded on the TOE host platforms. A.TRUSTED is covered by:

- ON.PHYCAL: Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack. This objective provides for the physical protection of the TOE hardware and software to protect against unauthorized access.
- ON.CREDEN: Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security. This objective supports this assumption by requiring protection of all authentication data.

Table 8-4 is included as a consistency check to show that all security objectives of the TOE map to at least one threat or organizational security policy.

Table 8-4 Reverse Mapping of Security Objectives of the TOE map to Threat/Policies

No.	Objective Name	Threat/Policy
1	O.PARTPROTCT	T.COMINT T.COMDIS T.PRIVIL P.MANAGE P.ACCESS
2	O.IDBLOCK	T.SCNCFG T.SCNMLC P.ANALYZ
3	O.IDSCAN	T.NOHALT T.SCNCFG T.SCNMLC T.SCNVUL P.DETECT
4	O.IDSENS	T.NOHALT T.MISUSE P.DETECT
5	O.IDANLZ	T.FALASC P.ANALYZ
6	O.EADMIN	T.IMPCON P.MANAGE
7	O.ACCESS	T.IMPCON T.COMDIS T.NOHALT P.MANAGE P.ACCESS
8	O.IDAUTH	T.COMINT T.COMDIS T.NOHALT T.PRIVIL T.IMPCON P.MANAGE P.ACCESS P.ACCACT
9	O.OFLOWS	T.INFLUX P.PROTCT

No.	Objective Name	Threat/Policy
10	O.AUDITS	T.FACCNT P.ACCACT P.DETECT
11	O.PARTINTEGR	T.COMINT P.INTGTY

Table 8-5 is included as a consistency check to show that all security objectives of the IT Environment map to at least one threat, organizational security policy, or assumption.

Table 8-5 Reverse Mapping of Security Objectives of the IT Environment to Threat/Policies/Assumptions

No.	Objective Name	Threat/Policy/Assumption
12	OE.COLLECTEVENTVULN	T.NOHALT T.SCNCFG T.SCNMLC T.SCNVUL P.DETECT
13	OE.OFLOWS	T.INFLUX P.PROTCT
14	OE.PARTINTEGR	T.PRIVIL
15	OE.PARTPROTCT	T.PRIVIL
16	OE.PROTCTCOMM	T.TRANSMIT
17	OE.TIME	T.COMINT T.COMDIS T.PRIVIL

Table 8-6 is included as a consistency check to show that all security objectives of the IT Environment map to at least one threat, organizational security policy, or assumption.

Table 8-6 Reverse Mapping of Security Objectives of the Non-IT Environment to Threat/Policies/Assumptions

Objective Name	Threat/Policy/Assumption
ON.INSTALL	P.MANAGE A.NOEVIL T.IMPCON
ON.PHYCAL	A.NOEVIL A.PROTCT A.TRUSTED P.PROTCT
ON.CREDEN	P.MANAGE A.NOEVIL A.TRUSTED
ON.PERSON	P.MANAGE A.DYNAMIC A.MANAGE
ON.INTROP	A.ACCESS A.DYNAMIC

Objective Name	Threat/Policy/Assumption
	A.SCOPE
ON.EXPORT	T.COMDIS
ON.PASSWD	A.PASSWD
ON.PRTCTCOMM	A.PROTCTCOMM

8.2 Security Requirements Rationale

8.2.1 Functional Requirements

Table 8-7 shows that all of the security objectives of the TOE are satisfied.

Table 8-7 All Objectives Met by Functional Components

Item	Objective	Security Functional Requirement	Component Name
1	O.PARTPROTCT	FMT_MTD.1*	Management of TSF data
		FPT_RVM_EXP.1	Non-bypassability of the TSP
		IDS_STG_EXP.1-1	Guarantee of Defense perspective data Availability
2	O.IDBLOCK	IDS_SR_EXP.1	Security response
3	O.IDSCAN	IDS_DPD_EXP.1	Defense perspective data collection
4	O.IDSENS	IDS_DPD_EXP.1	Defense perspective data collection
		IDS_SA_EXP.1	Security alarms
		IDS_SR_EXP.1	Security response
5	O.IDANLZ	IDS_ANL_EXP.1	Analyzer analysis
6	O.EADMIN	FIA_ATD.1*	User attribute definition
		FAU_SAR.1	Audit review
		FMT_MTD.1*	Management of TSF data
		FMT_SMF.1	Specification of management functions
		FMT_SMR.1	Security roles
		IDS_RDR_EXP.1	Restricted data review
		IDS_DRS_EXP.1	Data Reporting
7	O.ACCESS	FAU_SAR.2	Restricted audit review
		FIA_UAU.2	User authentication before any action
		FIA_UID.2	User identification before any action
		FMT_MTD.1*	Management of TSF data
		IDS_RDR_EXP.1	Restricted Data Review
		IDS_STG_EXP.1-1	Guarantee of Defense perspective data Availability

Item	Objective	Security Functional Requirement	Component Name
8	O.IDAUTH	FIA_UAU.2	User authentication before any action
		FIA_UID.2	User identification before any action
		FIA_SOS.1	Verification of secrets
9	O.OFLOWS	IDS_STG_EXP.1-1	Guarantee of Defense perspective data Availability
10	O.AUDITS	FAU_LOG_EXP.1	Audit log generation
		FAU_GEN.2	User identity association
11	O.PARTINTEGR	IDS_STG_EXP.1-1	Guarantee of Defense perspective data Availability

O.PARTPROTCT: The TOE when invoked by the underlying host OS must protect itself from unauthorized modifications and access to its functions and data within the TOE, through its own interfaces O.PARTPROTCT is addressed by:

- FMT_MTD.1* Management of TSF data, which specifies the management of TSF Data according to assigned roles.
- FPT_RVM_EXP.1 Non-bypassability of the TSP, which requires that TSP enforcement functions are invoked and succeed before a security-relevant function is allowed to proceed.
- IDS_STG_EXP.1-1 Guarantee of Defense perspective data Availability, the TOE shall protect the stored defense perspective data from unauthorized deletion and modification.

O.IDBLOCK: The TOE must block network security threats or out-of-policy applications.

- IDS_SR_EXP.1 Security response, which requires the TSF to take specified actions based upon the equipment and location of a detected threat.

O.IDSCAN: The TOE must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System. O.IDSCAN is addressed by:

- IDS_DPD_EXP.1 Defense perspective data collection, which requires that the TOE be able to collect specified information from targeted IT System resource(s).

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

- IDS_DPD_EXP.1 Defense perspective data collection, which requires that the TOE be able to collect specified information from targeted IT System resource(s).
- IDS_SA_EXP.1 Security alarms, which requires the TSF to take action to send an alert to the QRadar console, send the alert to the syslog, or send a notification via e-mail upon detection of a potential security violation
- IDS_SR_EXP.1 Security response, which requires the TSF to take specified actions based upon the equipment and location of a detected threat.

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

- IDS_ANL_EXP.1 Analyzer analysis, which requires the TOE to perform statistical, signature, and behavioral analysis function(s) on all IDS data received.

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

- FIA_ATD.1* User attribute definition, which requires that the TSF maintain security attributes of users.
- FAU_SAR.1 Audit review, which requires that the auditor be able to read audit records.
- FMT_MTD.1* Management of TSF data, which specifies the management of TSF Data according to assigned roles.
- FMT_SMF.1 Specification of management functions, which requires the TSF is capable of performing the specified security management functions.
- FMT_SMR.1 Security roles, which requires that the TSF maintain multiple administrative roles.
- IDS_RDR_EXP.1 Restricted data review, which requires the TOE to provide the authorized administrator with the capability to read all data from the defense perspective data, and in a manner suitable for the authorized administrator to interpret the information.
- IDS_DRS_EXP.1 Data reporting, which requires the TSF be able to report collected event data using automatically generated reports. In addition, the TSF is capable of generating user defined reports and real-time views.

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

- FAU_SAR.2 Restricted audit review, which requires the TSF to prohibit all users read access to the audit records, except those users that have been granted explicit read-access.
- FIA_UAU.2 User authentication before any action, which requires each user to be successfully authenticated before allowing access to the TOE.
- FIA_UID.2 User identification before any action, which requires that users be successfully identified before allowing access to the TOE.
- FMT_MTD.1* Management of TSF data, which specifies the management of TSF Data according to assigned roles.
- IDS_RDR_EXP.1 Restricted Data Review, which specifies the TOE shall provide the Administrator with the capability to read all data from the defense perspective data and in a manner suitable for the user to interpret the information.
- IDS_STG_EXP.1-1 Guarantee of Defense perspective data Availability, the TOE shall protect the stored Defense perspective data from unauthorized deletion and modification.

O.IDAUTH: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. O.IDAUTH is addressed by:

- FIA_UAU.2 User authentication before any action, which requires each user to be successfully authenticated before allowing access to the TOE.
- FIA_UID.2 User identification before any action, which requires that users be successfully identified before allowing access to the TOE.
- FIA_SOS.1 Verification of secrets, which requires that the TSF provide a mechanism to verify that secrets meet the specified password policy.

O.OFLOWS: The TOE must appropriately handle potential audit and defense perspective data storage overflows, through its own interfaces O.OFLOWS is addressed by:

- IDS_STG_EXP.1-1 Guarantee of Defense perspective data Availability, which requires the TOE shall protect the stored Defense Perspective data from unauthorized deletion and modification through its own TSFI, the TOE shall ensure that the most recent, limited by available storage space, defense perspective data will be maintained when defense perspective data storage exhaustion occurs, and the TOE shall send an alarm if the storage capacity has been reached..

O.AUDITS: The TOE must record audit records for accesses and use of the System blocking function. O.AUDITS is addressed by:

- FAU_LOG_EXP.1 Audit log generation, which requires the ability to audit specified events.
- FAU_GEN.2 User identity association, which requires the ability to associate an auditable event with a specific user.

O.PARTINTEGR: The TOE with the support of the underlying host OS must ensure the integrity of all audit and defense perspective data, through its own interfaces. O.PARTINTEGR is addressed by:

- IDS_STG_EXP.1-1 Guarantee of Defense perspective data Availability, the TOE shall protect the stored defense perspective data from unauthorized deletion and modification.

Table 8-8 is included as a consistency check to show that all SFRs map to Security Objectives of the TOE

Table 8-8 Reverse Mapping of SFRs to Objectives

No.	SFRs	Objectives
1.	FAU_LOG_EXP.1	O.AUDITS
2.	FAU_GEN.2	O.AUDITS
3.	FAU_SAR.1	O.EADMIN
4.	FAU_SAR.2	O.ACCESS
5.	FIA_ATD.1*	O.EADMIN
6.	FIA_SOS.1	O.IDAUTH
7.	FIA_UAU.2	O.IDAUTH O.ACCESS
8.	FIA_UID.2	O.IDAUTH O.ACCESS
9.	FMT_MTD.1*	O.PARTPROTCT O.EADMIN O.ACCESS
10.	FMT_SMF.1	O.EADMIN
11.	FMT_SMR.1	O.EADMIN
12.	FPT_RVM_EXP.1-1	O.PARTPROTCT
13.	IDS_DPD_EXP.1	O.IDSCAN O.IDSENS
14.	IDS_ANL_EXP.1	O.IDANLZ
15.	IDS_SA_EXP.1	O.IDSENS
16.	IDS_SR_EXP.1	O.IDBLOCK O.IDSENS
17.	IDS_RDR_EXP.1	O.EADMIN O.ACCESS
18.	IDS_STG_EXP.1-1	O.ACCESS O.OFLOWS O.PARTINTEGR O.PARTPROTCT
19.	IDS_DRS_EXP.1	O.EADMIN

8.2.2 Dependencies

Table 8-9 shows the dependencies between the functional requirements. All dependencies are satisfied. Dependencies that are satisfied by a hierarchical component are denoted by an (H) following the dependency reference. If the TOE dependency is met by an SFR in the IT environment an "E" will be next to the reference number. For the SFRs in Part 2 with a dependency on FAU_GEN.1, this dependency is satisfied by the explicit SFR FAU_LOG_EXP.1. The only difference is that FAU_LOG_EXP.1 does not require audit of startup and shutdown of the audit function.

Table 8-9 TOE Dependencies Satisfied

No.	Component	Component Name	Dependencies
1.	FAU_LOG_EXP.1	Audit log generation	FPT_STM.1
2.	FAU_GEN.2	User identity association	FAU_LOG_EXP.1
			FIA_UID.1
3.	FAU_SAR.1	Audit review	FAU_LOG_EXP.1
4.	FAU_SAR.2	Restricted audit review	FAU_SAR.1
5.	FIA_ATD.1*	User attribute definition	None
6.	FIA_SOS.1	Verification of secrets	None
7.	FIA_UAU.2	User authentication before any action	FIA_UID.1
8.	FIA_UID.2	User identification before any action	None
9.	FMT_MTD.1*	Management of TSF data	FMT_SMR.1
			FMT_SMF.1
10.	FMT_SMF.1	Specification of management functions	None
11.	FMT_SMR.1	Security roles	FIA_UID.1
12.	FPT_RVM_EXP.1-1	Non-bypassability of the TSP	None
13.	IDS_DPD_EXP.1	Defense perspective data collection	None
14.	IDS_ANL_EXP.1	Analyzer analysis	IDS_DPD_EXP.1
			IDS_EVD_EXP.1
			FPT_STM.1
15.	IDS_SA_EXP.1	Security alarms	IDS_ANL_EXP.1
16.	IDS_SR_EXP.1	Security response	IDS_ANL_EXP.1
17.	IDS_RDR_EXP.1	Restricted data review	IDS_DPD_EXP.1
			IDS_EVD_EXP.1
18.	IDS_STG_EXP.1-1	Guarantee of defense perspective data availability	IDS_DPD_EXP.1
			IDS_EVD_EXP.1
19.	IDS_DRS_EXP.1	Data reporting	IDS_DPD_EXP.1
			IDS_EVD_EXP.1

Table 8-10 IT Environment Dependencies are Satisfied

No	Component	Component Name	Dependencies
20.	FAU_STG_EXP.2	Guarantees of audit data availability	FAU_LOG_EXP.1
21.	FPT_RVM_EXP.1-1	Non-bypassability of the TSP	None
22.	FPT_SEP_EXP.1	TSF domain separation	None
23.	FPT_STM.1	Reliable time stamps	None
24.	FTP_ITC.1	Trusted path/channels	None

No	Component	Component Name	Dependencies
25.	IDS_STG_EXP.1-2	Prevention of Defense Perspective data loss	None
26.	IDS_EVD_EXP.1	Event and vulnerability data collection	None

8.2.3 Strength of Function

A strength of function level of SOF-Basic counters an attack level of low. The environment is one where the potential attacker is unsophisticated, with access to only standard equipment and public information about the product. A user password is required to be used when accessing the QRadar GUI. The recommended password policy for administrators, users, and Customer Support users is defined in the Administrator's guide.

8.2.4 Assurance Requirements

Evaluation Assurance Level EAL2 was chosen to provide a basic level of assurance due to the low level threat of malicious attacks.

8.2.5 Rationale that IT Security Requirements are Internally Consistent

The IT Security Requirements are internally consistent. There are no requirements that conflict with one another. When different IT security requirements apply to the same event, operation, or data there is no conflict between the security requirements. The requirements mutually support each other to apply to the event, operation, or data.

For auditing, each of the SFRs builds on the others. For example, FAU_LOG_EXP.1 details the auditable events generated by the TSF. FAU_GEN.2 provides for the TSF to associate each auditable event with the identity of the user that caused the event. FAU_SAR.1 states that the TSF shall provide the Siebel Administrator with the capability to read all audit information from the audit records. FAU_SAR.2 builds on FAU_SAR.1 by stating the TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access. IDS_STG_EXP.1-1 provides protection of the stored audit records from unauthorized deletion and modifications.

Login processing brings in elements of many requirements, but all in a complementary way. FIA_ATD.1* defines the security attributes belonging to administrators, Customer Support users, and users. FIA_SOS.1 specifies the password policy that user's password must comply with. This policy is supported in the IT environment by training users to use strong passwords. FIA_UID.2 requires the user to be identified before allowing any other operations and FIA_UAU.2 requires the user to be authenticated before allowing any other operations.

The management requirements (FMT_) are related to many of the mechanisms involved with other requirements. FMT_MTD.1* specifies the management of TSF Data according to assigned roles which are defined in FMT_SMR.1. FMT_SMF.1 specifies the security management functions of the TSF. In many cases, the other mechanisms will enforce the settings made through management functions. Installation mechanisms (see ADO_IGS.1) rely on management functions. The administrator guidance (see AGD_ADM.1) documents the management functions.

FPT_RVM_EXP.1-1 makes certain the TSP enforcement functions are invoked and succeed before any other functions within the TOE's Scope of Control are allowed to proceed.

The IDS requirements describe the intrusion detection system requirements of the TOE. IDS_DPD_EXP.1 requires the TOE to be able to collect the specified information. IDS_ANL_EXP.1 requires the TOE to perform statistical, signature, and behavioral analysis on all defense perspective data collected (IDS_DPD_EXP.1). IDS_SA_EXP.1 requires the TSF to send an alert to the Offence Manager view of the QRadar Console, syslog, pager, or via e-mail. IDS_SR_EXP.1 allows the TSF to take action based upon a detected threat. IDS_RDR_EXP.1 requires the TOE to provide the Administrator with the capability to read all data from the defense perspective data and in a manner

suitable for the user to interpret the information. IDS_STG_EXP.1-1 requires the TOE to protect the stored defense perspective data from unauthorized deletion and modification. In addition, it requires the TOE to overwrite the oldest stored defense perspective data and send an alarm if the storage capacity has been reached. IDS_DRS_EXP.1 requires the TSF to be able to report collected event data using automatically generated reports. In addition the TOE is capable of generating user defined reports and the following real-time views.

8.2.6 Explicitly Stated Requirements Rationale

A refinement adds additional detail and narrows the scope, but has to be iterated to meet the original scope of the SFR. FPT_RVM_EXP.1-1 had to be explicitly stated because it provides partial TOE self-protection while relying on the OS and Hardware platforms to provide the full protection. According to CCIMB RI#19, which states the following: “Where necessary to cover different aspects of the same requirement (e.g. identification of more than one type of user), repetitive use (i.e. applying the operation of iteration) of the same Part 2 components to cover each aspect is possible. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE and the supporting evidence for its evaluation need to satisfy in order to meet the security objectives for the TOE. Since the iterations of FPT_RVM_EXP.1 span both the TOE requirements and IT Environment, they must be explicitly stated. FPT_SEP_EXP.1 had to be explicitly stated because it applies only to the IT environment. FAU_STG_EXP.2 had to be explicitly stated because it describes measures taken in the IT Environment to protect audit data stored in the IT Environment.

FAU_LOG_EXP.1 had to be explicitly stated, because the TOE does not provide the ability to audit of startup and shutdown of the audit function as required by FAU_GEN.1. However, in the TOE the audit capability is always enabled, and, since the TOE does audit startup and shutdown of the TOE, the auditing of startup or shutdown of the TOE is logically equivalent to startup or shutdown of the audit function.

A family of IDS requirements was created to specifically address the data collected and analyzed by an IDS. 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. IDS_DPD_EXP.1 had to be explicitly stated because there is not an existing SFR in the CC Part 2 that describes defense perspective data collection function. IDS_ANL_EXP.1 had to be explicitly stated because there is not an existing SFR in the CC Part 2 that describes an analyzer analysis function. IDS_SA_EXP.1 had to be explicitly stated because there is not an existing SFR in the CC Part 2 that describes send an alert generated in response to the data collected and analyzed by an IDS. IDS_SR_EXP.1 had to be explicitly stated because there is not an existing SFR in the CC Part 2 that describes a security response function. IDS_RDR_EXP.1 had to be explicitly stated because there is not an existing SFR in the CC Part 2 that describes a restricted data review function. IDS_STG_EXP.1-1 had to be explicitly stated because there is not an existing SFR in the CC Part 2 that describes the protection of data from unauthorized deletion other than audit data. IDS_DRS_EXP.1 had to be explicitly stated because there is not an existing SFR in the CC Part 2 that describes reporting of the data collected and analyzed by an intrusion detection system. IDS_EVD_EXP.1 had to be explicitly stated because there is not an existing SFR in the CC Part 2 that describes collection of information from targeted IT system resources.

8.2.7 Requirements for the IT Environment

Table 8-11 shows that all of the security objectives for the IT environment are satisfied. Rationale for each objective is included below the table.

Table 8-11 All Objectives for the IT Environment map to Requirements in the IT environment

Item	IT Environment Objective	IT Environment Objective Description	IT Environment SFR
12	OE.COLLECTEVENTVULN	The IT Environment must collect event and vulnerability data of an IT System	IDS_EVD_EXP.1
13	OE.OFLOWS	The IT Environment must appropriately handle potential audit and defense perspective data storage overflows, through the IT Environment's interfaces	FAU_STG_EXP.2 IDS_STG_EXP.1-2
14	OE.PARTINTEGR	The IT Environment must ensure the integrity of all audit and defense perspective data, through the IT Environment's interfaces within its scope of control.	FAU_STG_EXP.2 IDS_STG_EXP.1-2
15	OE.PARTPROTCT	The IT Environment must protect itself from unauthorized modifications and access to its functions and data within the TOE, through the IT Environment's interfaces within its scope of control.	FPT_RVM_EXP.1-2 FPT_SEP_EXP.1
16	OE.PROTCTCOMM	The IT environment must protect communications between the TOE and its components.	FTP_ITC.1
17	OE.TIME	The underlying operating system will provide reliable time stamps.	FPT_STM.1

OE.COLLECTEVENTVULN: The IT Environment must collect event and vulnerability data of an IT System. OE.COLLECTEVENTVULN is addressed by:

- IDS_EVD_EXP.1 Event and vulnerability data collection, which requires the IT Environment to collect the following information from the targeted IT System resource(s): event data from network devices that produce Netflow, Jflow, and Sflow events, and vulnerability data.

OE.OFLOWS: The IT Environment must appropriately handle potential audit and defense perspective data storage overflows, through the IT Environment's interfaces OE.OFLOWS is addressed by:

- FAU_STG_EXP.2 Guarantees of audit data availability, which requires that the IT Environment protect the stored audit records from unauthorised deletion and modifications.
- IDS_STG_EXP.1-2 Guarantee of Defense perspective data Availability, the IT Environment shall protect the stored defense perspective data from unauthorized deletion and modification.

OE.PARTINTEGR: The IT Environment must ensure the integrity of all audit and defense perspective data, through the IT Environment's interfaces within its scope of control. OE.PARTINTEGR is addressed by:

- FAU_STG_EXP.2 Guarantees of audit data availability, which requires that the IT Environment protect the stored audit records from unauthorised deletion and modifications.
- IDS_STG_EXP.1-2 Guarantee of Defense perspective data Availability, the IT Environment shall protect the stored defense perspective data from unauthorized deletion and modification.

OE.PARTPROTCT: The IT Environment must protect itself from unauthorized modifications and access to its functions and data within the TOE, through the IT Environment's interfaces within its scope of control. OE.PARTPROTCT is addressed by:

- FPT_RVM_EXP.1-2 Non-bypassability of the TSP, which requires that the IT Environment ensures the OS enforcement functions are invoked and succeed before a security-relevant function is allowed to proceed.
- FPT_SEP_EXP.1 TSF domain separation, which requires the Operating System to maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects initiating actions through the Operating System's Interface. The IT environment will enforce separation between security domains of subjects in the Operating System's Scope of Control.

OE.PROTCTCOMM: The IT environment must protect communications between the TOE and its components. OE.PROTCTCOMM is addressed by:

- FTP_ITC.1 Inter-TSF trusted channel, which requires the IT environment to provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

OE.TIME: The underlying operating system will provide reliable time stamps. OE.Time is addressed by:

- FPT_STM.1 Reliable time stamps, which require that time stamps be provided by the IT environment.

Table 8-12 Reverse Mapping of Security Requirements for the Environment to IT Security Objectives of the Environment

No.	IT Environment SFR	IT Environment Security Objective
22	FAU_STG_EXP.2	OE.PARTINTEGR OE.OFLOWS
23	FPT_RVM_EXP.1-2	OE.PARTPROTCT
24	FPT_SEP_EXP.1	OE.PARTPROTCT
25	FPT_STM.1	OE.TIME
26	FTP_ITC.1	OE.PROTCTCOMM
27	IDS_STG_EXP.1-2	OE.PARTINTEGR OE.OFLOWS
28	IDS_EVD_EXP.1	OE.COLLECTEVENTVULN

8.3 TOE Summary Specification Rationale

8.3.1 IT Security Functions

Table 8-13 shows that the IT Security Functions in the TOE Summary Specification (TSS) address all of the TOE Security Functional Requirements.

Table 8-13 Mapping of Functional Requirements to TOE Summary Specification

No	Functional Component	Functional Requirement	Requirement is met by:	
			Security Function Ref. No	Rationale
1	FAU_LOG_EXP.1	Audit log generation	AU-1	Specifies the types of events to be audited.
2	FAU_GEN.2	User identity association	AU-2	Specifies that each auditable event is associated with the identity of the user that caused the event.

No	Functional Component	Functional Requirement	Requirement is met by:	
			Security Function Ref. No	Rationale
3	FAU_SAR.1	Audit review	AU-3	Specifies the authorized administrator has the capability to read all audit information from the audit records.
4	FAU_SAR.2	Restricted audit review	AU-4	Specifies that only specific users have read access to the audit records.
5a	FIA_ATD.1-1	User attribute definition	IA-1	Specifies the security attributes maintained for Customer Support and administrator user.
5b	FIA_ATD.1-2	User attribute definition	IA-2	Specifies the security attributes maintained for each user.
6	FIA_SOS.1	User authentication	IA-3	Specifies that QRadar has a password policy.
7	FIA_UAU.2	User authentication before any action	IA-3	Specifies that the QRadar Administrator Interface requires each user to successfully authenticate with a password before being allowed any other actions.
8	FIA_UID.2	User identification before any action	IA-4	Specifies that the QRadar Administrator Interface requires each user to identify himself/herself before being allowed to perform any other actions.
9a	FMT_MTD.1-1	Management of TSF data	SM-1	Specifies that the TOE restricts the ability to access data regarding the Administration of Security Functions.
9b	FMT_MTD.1-2	Management of TSF data	SM-2	Specifies that the TOE restricts the ability to access data regarding Users with Privileges.
9c	FMT_MTD.1-3	Management of TSF data	SM-3	Specifies that the TOE restricts the ability to access data regarding Users sharing privileges.
9d	FMT_MTD.1-4	Management of TSF data	SM-4	Specifies that the TOE restricts the ability to access data regarding Customer Support Users.
9e	FMT_MTD.1-5	Management of TSF data	SM-5	Specifies that the TOE restricts the ability to access data regarding the management of passwords.
10	FMT_SMF.1	Specification of Management Functions	SM-6	Specifies the security management functions provided by the TOE.
11	FMT_SMR.1	Security roles	SM-7	Specifies the roles maintained in the TOE.

No	Functional Component	Functional Requirement	Requirement is met by:	
			Security Function Ref. No	Rationale
12	FPT_RVM_EXP.1-1	Non-bypassability of the TSP	SP-1	Specifies that the TSF ensures that the TSP enforcement functions are invoked and succeed before each function is allowed to proceed.
13	IDS_DPD_EXP.1	Defense perspective data collection	IDS-1	Specifies that the TOE collects the specified defense perspective data.
14	IDS_ANL_EXP.1	Analyzer analysis	IDS-2	Specifies that the TOE performs statistical, signature, and behavioral analysis on all IDS data received.
15	IDS_SA_EXP.1	Security alarms	IDS-3	Specifies that an alert will be sent upon detection of a potential security violation.
16	IDS_SR_EXP.1	Security response	IDS-4	Specifies that the TSF will take action when a threat is detected.
17	IDS_RDR_EXP.1	Restricted Data Review	IDS-5	Specifies that the TOE provide the administrator with the capability to read all data from the defense perspective data and in a manner suitable for the user to interpret the information.
18	IDS_STG_EXP.1-1	Guarantee of Defense perspective data Availability	IDS-6	Specifies that the TOE will protect stored defense perspective data from unauthorized deletion and modification. In addition, that the TOE will overwrite the oldest stored defense perspective data and send an alarm if the storage capacity is exceeded.
19	IDS_DRS_EXP.1	Data Reporting	IDS-7	Specifies that the TSF be able to collect event data using automatically generated reports. In addition, the TSF is capable of generating user defined reports and real-time views.

8.3.2 Assurance Measures

The assurance measures rationale shows how all assurance requirements are satisfied. The rationale is provided in Table 8-14.

Table 8-14 Assurance Measures Rationale

Component	Evidence Requirements	How Satisfied	Rationale
ACM_CAP.2	CM Documentation • CM Proof • Configuration Item List	A Configuration list was provided	• CM Proof - Show proof that CM system is being used for development. • Configuration Item List(s) - is comprised of a list of the source code files and version numbers - is comprised of a list of design documents with version numbers - is comprised of test documents with version numbers - user and administrator documentation with version numbers
ADO_DEL.1	Delivery Procedures	Delivery procedures were provided	Provides a description of all procedures that are necessary to maintain security when distributing software to the user's site. - Applicable across all phases of delivery from packaging, storage, distribution
ADO_IGS.1	Installation, generation, and start-up procedures	An Installation Guide was provided	Provides detailed instructions on how to install the product.
ADV_FSP.1	Functional Specification	A Functional Specification was provided	Provides rationale that TSF is fully represented
			Describes the TSF interfaces and TOE functionality
			Describes TOE functionality
ADV_HLD.1	High-Level Design	A High Level Designs was provided	Describes the TOE subsystems and their associated security functionality
ADV_RCR.1	Representation Correspondence	Documentation was provided that includes correspondence analysis between: 1. TSS and functional specification; 2. functional specification and high-level design; 3. high-level design and the low-level design; and 4. low-level design and implementation representation subset.	Provides the following two dimensional mappings: 1. TSS and functional specification; 2. functional specification and high-level design.
AGD_ADM.1	Administrator Guidance	An Administrator Guide was provided.	Describes how to administer the TOE securely.

Component	Evidence Requirements	How Satisfied	Rationale
AGD_USR.1	User Guidance	Not applicable for this product	Describes the secure use of the TOE.
ATE_COV.1	Test Coverage Analysis	Test Coverage was provided	Shows correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_FUN.1	Test Documentation	Test Documentation (Test Plans) provided	Test documentation includes test plans and procedures and expected and actual results.
ATE_IND.2	TOE for Testing	TOE for Testing	The TOE was provided for testing.
AVA_SOF.1	SOF Analysis	SOF Analysis was reviewed.	Provides a rationale that each mechanism identified in the ST as having an SOF meets or exceeds the minimum strength level specified there.
AVA_VLA.1	Vulnerability Analysis	Vulnerability Analysis was reviewed	Provide an analysis of the TOE deliverables for obvious ways in which a user can violate the TSP, including the disposition of obvious vulnerabilities.

8.4 PP Claims Rationale

Not applicable. There are no PP claims.

9 Appendix

9.1 Acronyms

Table 9-1 Acronyms

Acronym	Definition
ACM	Configuration Management
ADO	Delivery and Operation
ADV	Development
AGD	Guidance Documents
ALC	Life cycle support
ATE	Tests
AVA	Vulnerability assessment
CC	Common Criteria [for IT Security Evaluation]
DSM	Device Support Module
EAL	Evaluation Assurance Level
FAU	Security Audit
FCO	Communication
FCS	Cryptographic Support
FDP	User Data Protection
FIA	Identification and Authentication
FMT	Security Management
FPT	Protection of the TSF
FTA	TOE Access
FTP	Trusted Channels/Path
GUI	Graphical User Interface
ID	Identifier
IDS	Intrusion Detection System
IT	Information Technology
NIDS	Network Intrusion Detection System
NMAP	Open Source Network Mapper
SF	Security Function
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy
VA	Vulnerability Assessment

9.2 References

Table 9-2 References

Common Criteria for Information Technology Security Evaluation, CCIMB-2004-01-002, Version 2.2, January 2004.
QRadar 3.0 Administrator Guide Document release v5.1.1 July, 2006
QRadar 3.0 User Guide Document release v5.1 May, 2006
QRadar Installation Guide, release v5.1 May, 2006
QRadar Hardware Installation Guide, release v5.1 May, 2006
Getting Started Guide, release v5.1 May, 2006

9.3 Glossary

Table 9-3 Customer Specific Terms

Term	Definition
Alert	Once the defense perspective data is analyzed by correlating the event with the various types of raw data, normalized data, and Offences, then weighted Offence alerts can be generated.
Block	Prevent network traffic from moving through the network.
Customer network	The domain of network and host traffic to be analyzed by the TOE.
Defense Perspective Data	The complete set of information provided on the customer network which includes: flow information, event collection information, and general analysis data generated by the TSF.
Device Support Module	A DSM is a multi-faceted capability of the Event Collector and Event Processor to collect, normalize, and preprocess incoming events. (Note: The DSM is to be considered as something to be "plugged in" and the actual amount of DSMs that can be accessed is unlimited. (These DSMs are outside of the TOE.)
Offence Manager	The Offence Manager is the name given to the GUI screen tab menu option view (interface) to the core processing component that implements the Judicial System Logic (JSL), specifically the Magistrate sub component of the Engine component of the TOE. The JSL is the foundation for event processing and correlation in the Offence Manager view.
External event device	An external IT Entity network device that provides the TOE external event data (traps or events) and vulnerability data for analysis to detect threats, and/or receives from the TOE blocking data (to fill in) to prevent the threat from proliferating throughout the network.
External event information	The aggregated and normalized data provided by the external event devices. Also referred to as part of Defense Perspective data.
Flow	A single stream of related data packets.
Flow information	The aggregated and normalized flow data collected by the QFlow Collectors.
IDS data	Intrusion Detection System data that is made up of defense perspective data, alerts, blocks generated by the TSF, and any configuration data related to these. Also referred to as part of Defense Perspective data.
Raw normalized event data	Raw normalized event data is collected from a device and transformed onto a well –known processing format and stored in the appropriate Raw Normalized Event Storage proprietary database.

Term	Definition
Offence Model	The Offence Model is a relational database that stores a variety of data displayed in the Offence Manager view. These include Rap Sheet analysis, Defense Perspective analysis, Custom Rules Engine (Offences), Offence Describer and analysis, Offence Statistics, Worm Propagation/Offence Chaining analysis, and Judgment modules data.
Security Management Data	TOE configuration data and audit data.
Surveillance information	Includes a database of flow information, a set of analysis data, and a database of external event information.
Violations	Violations are generated by the TSF and are the results of the analysis of the Defense Perspective Data.

Table 9-4 CC Specific Terms

Term	Definition
Authorised user	A user who may, in accordance with the TSP, perform an operation.
External IT entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.