Q1 Labs, Inc. QRadar Release 7.0.0
Security Target

Version 1.2
July 15, 2010

Prepared for:
Q1 Labs, Inc.
890 Winter Street
Suite 230
Waltham, MA 02451 USA

Prepared by:
Booz Allen Hamilton
Common Criteria Testing Laboratory
900 Elkridge Landing Road, Suite 100
Linthicum, MD 21090-2950

Table of Contents

List of Figures

List of Tables

1 Security Target Introduction

This chapter presents the Security Target (ST) identification information and an overview. An ST contains the Information Technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by the TOE.

1.1 ST Reference

This section provides information needed to identify and control this ST and its Target of Evaluation. This ST targets Evaluation Assurance Level 3 (EAL3).

1.1.1 ST Identification

ST Title:	Q1 Labs, Inc. QRadar Release 7.0.0 Security Target
ST Version:	1.2
ST Publication Date:	July 15, 2010
ST Author:	Booz Allen Hamilton

1.1.2 Document Organization

Chapter 1 of this ST provides identifying information for the TOE. It includes an ST Introduction, ST Reference, ST Identification, TOE Reference, TOE Overview, and TOE Type.

Chapter 2 describes the TOE Description, which includes the physical and logical boundaries, and describes the components and/or applications that are excluded from the evaluated configuration.

Chapter 3 describes the conformance claims made by this ST.

Chapter 4 describes the Security Problem Definition as it relates to threats, Operational Security Policies, and Assumptions met by the TOE.

Chapter 5 identifies the Security Objectives of the TOE and of the Operational Environment.

Chapter 6 describes the Extended Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs).

Chapter 7 describes the Security Functional Requirements.

Chapter 8 describes the Security Assurance Requirements.

Chapter 9 is the TOE Summary Specification (TSS), a description of the functions provided by the TOE to satisfy the SFRs and SARs.

Chapter 10 is the Security Problem Definition Rationale and provides a rationale or pointers to a rationale, for security objectives, assumptions, threats, requirements, dependencies, and PP claims for the chosen EAL, any deviations from CC Part 2 concerning SFR dependencies, and a mapping of threats to assumptions, objectives, and

SFRs. It also identifies the items used to satisfy the Security Assurance Requirements for the evaluation.

1.1.3 Terminology

This section defines the terminology used throughout this ST. The tables below are to be used by the reader as a quick reference guide for terminology definitions.

Terminology	Definition
Administrator	A user that has all of the Admin extended privileges enabled for their account via roles.
Alert	A message sent or event generated in response to a monitored condition. For example, an alert informs a user if a policy has been breached or the network is under attack.
Analyzer	See Intrusion Detection System Analyzer.
Analyzer Data	IDS data collected by the Analyzer functions
Analyzer Functions	The active part of the Analyzer responsible for performing intrusion analysis of information that may be representative of vulnerabilities in and misuse of IT resources, as well as reporting of conclusions.
Asset	Information or resources (servers and hosts) to be protected by the countermeasures of a TOE.
Asset Profile	Displays the services running on each asset gathered from vulnerability assessment solutions and or network activity (flow) data. The profile data is used for correlation purposes to reduce false positives.
Attack	An attempt to bypass security controls on an IT System. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the IT System and the effectiveness of existing countermeasures.
Audit	The independent examination of log events and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend indicated changes in controls, policy, or procedures.
Audit Data	In an IT System, a chronological log of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized. All audit data is captured in audit events. The term audit event is synonymous with audit record.
Audit Record	See Audit data.
Authentication	To establish the validity of a claimed user or object.
Authorized Administrator	A subset of authorized users that manage an IDS component.
Authorized User	A user that is allowed to perform IDS functions and access data
Availability	Assuring information and communications services will be ready for use when expected.
Behavior	Indicates the normal manner in which the system or network functions or operates.
Category	Contains the name, magnitude, local target count, events, and last event of a specific offense.
Checkpoint LEA	Product that extracts IT data logs from Checkpoint firewalls.
Classless Inter-Domain Routing	CIDR is an addressing scheme for the Internet, which allocates and specifies Internet addresses used in inter-domain routing. With CIDR, a single IP address can be used to designate many unique IP addresses.
Client	The host that originates communication.
Compromise	An intrusion into an IT System where unauthorized disclosure, modification or destruction of sensitive information may have occurred.

Confidentiality	Assuring information will be kept secret, with access limited to appropriate persons.
Console	See QRadar Console.
Content Capture	QFlow Collectors capture a configurable amount of payload and store the data in the flow logs. A user can view this data using the View Flows function.
Credibility	The credibility of this offense, as determined by the credibility rating from source devices. For example, credibility is increased when multiple sources report the same event.
Custom Rules Engine	Determines the custom rules to apply to an event in determining if an offense has occurred.
Deployment Editor	The deployment editor allows administrators to manage the individual subsystems of a QRadar deployment. Once the Flow, Event, and System Views are configured, administrators can access and configure the individual subsystems of each managed host. Note: The Deployment Editor requires Java Runtime Environment.
Device Support Module	Allows you to integrate the TOE with external devices in a network. Through the user interface users configure Log Sources to use the appropriate DSMs to enable the collection and parsing of events which are processed through the QIDmap for the intended log source and Normalized. Using the event mapping tool, an administrator can map a normalized or raw event to another event description and category if they so wish. Event mapping also allows the user to map unknown log source events to be displayed, categorized and correlated appropriately.
End User	Someone who belongs to a non-administrative role. The privileges assigned to this role are defined by the administrator.
Event	Record from a device that describes an action on a network or host. The events in the evaluated configuration include the following: SOAP, Syslog (TCP), Syslog (UDP), JDBC/ODBC, SNMP, NSM, Lea, Cisco SDEE, and Log file protocol.
Event Collector	Component of the Event Processor. Collects security events and log messages from various types of security devices in a network. The Event Collector gathers events or logs from local, remote, and device sources. The Event Collector then normalizes the logs and events and sends the information to the Event Processor.
Event Processor	Processes events/log messages collected from its Event Collector. The events are bundled once again to conserve network usage. Once received, the Event Processor correlates the logs in real time for association to offenses. The Event processor also provides distributed storage of event and log data.
Extended Privilege	A privilege that requires another privilege to be given before it can be given.
External IT Product	In the evaluated configuration, the External IT product is the Internet that the TOE connects to in order to receive patch and/or IDS definition updates on event and vulnerability mappings through the auto-update service provided by Q1 Labs.
Flow	Communication session between two devices. Describes how traffic is communicated, what was communicated (if content capture option has been selected), and includes such details as when, who, how much, protocols, priorities, options, etc. Flow data refers to: Specific properties of a flow including: IP addresses, ports, protocol, bytes, packets, flags, direction, and application ID.

	Flow logs refer to: Record of flows that enables the system to understand the context of a particular transmission over the network. Flow data is a type of IDS data.
Flow Sources	Source of flows that the QFlow Collector receives. Using the deployment editor, one can add internal and external flow sources from the System or Flow Views in the deployment editor.
Flow Type View	Allows one to view network activity according to flow types. This depends on the ratio of incoming activity to outgoing activity.
IDS Data	Synonymous with System data.
Integrity	Assuring information will not be accidentally or maliciously altered or destroyed.
Internet Protocol	IP is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other systems on the Internet. An IP address includes a network address and a host address. An IP address can also be divided by using classless addressing or subnetting.
Interval	The default time period in the system. Affects the update intervals of the graphs and how much time each flow log file contains.
Intrusion	Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.
Intrusion Detection	Pertaining to techniques which attempt to detect intrusion into an IT System by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.
Intrusion Detection System	A combination of Sensors, Scanners, and Analyzers that monitor an IT System for activity that may inappropriately affect the IT System's assets and react appropriately.
Intrusion Detection System Analyzer	The component of an IDS that accepts IDS data from Sensors, Scanners and other IT System resources, and then applies analytical processes and information to derive conclusions about intrusions (past, present, or future).
Intrusion Detection System Component	A Sensor, Scanner, or Analyzer.
Intrusion Detection System Scanner	The component of an IDS that collects static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.
Intrusion Detection System Sensor	The component of an IDS that collects real-time events that may be indicative of vulnerabilities in or misuse of IT resources.
JFlow	A proprietary accounting technology used by Juniper® Networks that allows users to collect IP traffic flow statistics. J-Flow enables users to export data to a UDP ort on a J-Flow collector.
Layer 7	A layer of the OSI model that supports application and end-user processes. This layer provides application services for file transfers, e-mail, and other network software services.
Logic Unit	Sentry component that includes specific algorithms used to test objects.
Log source	An external IT product that forwards formulated logs to the TOE for processing.
Magistrate	Component of the Console. The Magistrate provides views, reports, alerts, and analysis of network traffic and security events. The Magistrate processes the event against the defined custom rules to create an offense.
Magnitude	Specifies the relative importance of the offense and is a weighted value calculated from the Relevance, Severity, and Credibility. The magnitude bar

	in the Offenses interface and Dashboard provides a visual representation of all correlated variables of the offense, attacker, target, or network. The magnitude of an offense is determined by several tests that performed on an offense every time it has been scheduled for re-evaluation, usually because events have been added or the minimum time for scheduling has occurred.
Managed host	A managed host is a system in a deployment that has QRadar software installed.
NetFlow	A proprietary accounting technology developed by Cisco Systems® Inc. that monitors traffic flows through a switch or router, interprets the client, server, protocol, and port used, counts the number of bytes and packets, and sends that data to a NetFlow collector. A user can configure QRadar to accept Network Data Exports (NDE's) and thus become a NetFlow collector. The TOE understands NDE’s for version 1, 5, 7, and 9.
Network	Two or more machines interconnected for communications.
Offense	Includes multiple events from one host. An offense is an incident that has been processed through QRadar using multiple inputs, individual events, and events combined with analyzed behavior and vulnerabilities.
Packet	A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.
Packeteer	Packeteer is a 3rd party data source that collects, aggregates, and stores network performance data. Once an external flow source is configured for Packeteer, one can send flow information from a Packeteer device to QRadar.
Payload	Within an event, this specifies the payload of the event that the log describes.
Permission	See privilege.
Privilege	Privileges are bundled into roles and applied to Users. Users can be assigned these to access different parts and functions of the TOE. The following are the main privileges associated with QRadar: Admin, Offenses, Log Activity, Assets, Resolution, Network Activity, and Reports.
Protocol	A set of rules and formats that determines the communication behavior of layer entities in the performance of the layer functions. It may still require an authorization exchange with a policy module or external policy server prior to admission.
QFlow Collector	Collects ISD data from devices and various live or recorded data feeds, such as network taps, span/mirror ports, NetFlow, and QRadar flow logs.
QRadar Console	Web interface for QRadar. QRadar is accessed from a standard web browser (Internet Explorer 7.0 or Mozilla Firefox 3.6). When accessing the system, a prompt appears for a user name and password, which must be configured in advance by the QRadar administrator.
QRadar Identifier	QID is a mapping of a single event of an external device to a Q1 Labs unique identifier.
Relevance	Relevance determines the impact on a network of an event, category, or offense. For example, if a certain port is open, the relevance is high.
Remote Trusted IT Product	In the evaluated configuration, a remote trusted IT product is a TOE component that is installed on a separate machine. All TOE components are installed on separate machines in the evaluated configuration.
Reports	A function that creates executive or operational level charting representations of network and security activity.
Resolver	A Resolver executes assigned Resolver Actions.
Resolver Action	A Resolver Action blocks host(s) affecting a network. A Resolver Action can have several Resolvers assigned as primary or reserve Resolvers.
Resolver Type	Specifies the type of Resolver. QRadar pushes out resolver actions to the

	following devices: TCP Reset, ARP Redirect, Cisco, Cisco PIX, NetScreen Firewall, Juniper router, and Checkpoint Firewall Resolver.
Role	A set of privileges specified by an Administrator. Roles are applied to users.
Rule	Collection of conditions and consequent actions. A user can configure rules that allow QRadar to capture and respond to specific event and or flow sequences. The rules allow a user to detect specific, specialized events and forward notifications to either the Offense interface or log file, e-mail a user, or resolve the event or offense, if the Resolution option is active.
Scanner	See Intrusion Detection System Scanner.
Scanner Data	IDS data collected by the Scanner functions.
Scanner Functions	The active part of the Scanner responsible for collecting configuration information that may be representative of vulnerabilities in and misuse of IT resources (i.e., Scanner data).
Security	A condition that results from the establishment and maintenance of protective measures that ensures a state of inviolability from hostile acts or influences.
Security Information Management (SIM)	SIM is a general IT system concept that involves a distributed environment of machines that generate output. Within SIM, machines can be configured to send outputs to a centralized system for aggregation purposes. SIM is used in the TOE to refer to the ability for Managed Hosts to send data to the Console for correlation and aggregation.
Security Policy	The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
Sensor	See Intrusion Detection System Sensor.
Sensor Data	IDS data collected by the Sensor functions.
Sensor Functions	The active part of the Sensor responsible for collecting information that may be representative of vulnerabilities in and misuse of IT resources (i.e., Sensor data).
Severity	The severity of an offense. Severity indicates the amount of threat than an attacker poses in relation to how prepared the target is for the attack. This value is directly mapped to the event category that correlates to the offense. For example, a Denial of Service (DoS) attack is always has a severity of 10, which indicates a severe occurrence.
SFlow	A multi-vendor and end-user standard for sampling technology that provides continuous monitoring of application level traffic flows on all interfaces simultaneously. sFlow combines interface counters and flow samples into sFlow datagrams that are sent across the network to an sFlow collector. QRadar supports sFlow versions 2, 4, and 5.
Simple Network Management Protocol	SNMP is a network management protocol used to monitor IP routers, other network devices, and the networks to which they attach.
Subnet	A network subdivided into networks or subnets. When subnetting is used, the host portion of the IP address is divided into a subnet number and a host number. Hosts and routers identify the bits used for the network and subnet number through the use of a subnet mask.
Superflows	Multiple flows with the same properties are combined into one flow to increase processing by reducing storage.
System Administrator	System Administrators can only configure IDS data collection standards/protocols and basic QRadar functionality. However, System Administrators cannot edit user accounts, with the exception of changing their own password.
System Data	Network traffic and host profile information that is collected by the TOE.
System Log	This log is used to capture alerts sent by the system when an intrusion is detected.

TOE Security Functions	TSF is a set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
TOE Security Policy	A set of rules that regulate how assets are managed, protected, and distributed within a TOE.
Transmission Control Protocol	TCP is a reliable stream service that operates at the transport-layer Internet protocol, which ensures successful end-to-end delivery of data packets without error.
Transmission Control Protocol Flags	A type of marker that can be added to a packet to alert the system of abnormal activity. Only a few specific combinations of flags are valid and typical, in normal traffic. Abnormal combinations of flags often indicate an attack or an abnormal network condition.
Transmission Control Protocol Resets	For TCP-based applications, QRadar can issue a TCP reset to either the client or server in a conversation. This stops the communications between the client and the server.
User	Any user of the TOE with one of the following roles: Administrator, System Administrator, or End User.
User Data	User data refers to data captured during the following processes by all users of the TOE: identification and authentication and management functions.
Violation	Includes a violation of corporate policy.

Table 1-1: Customer Specific Terminology

Term	Definition
Authorized user	A user who may, in accordance with the TSP, perform an operation. This is an end user or an administrator.
External IT entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
IT Product	A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.
Protection Profile	An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.
Role	A predefined set of rules establishing the allowed interactions between an end user and the TOE.
Security Target	A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
Target of Evaluation	The TOE is an IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.
Threat	The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. A potential violation of security.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
TSF Data	Data created by and for the TOE, which might affect the operation of the TOE.
TOE Security Functions (TSF) Scope of Control	TSC is the set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Table 1-2: CC Specific Terminology

1.1.4 Acronyms

The acronyms used throughout this ST are defined in Table 1-3: Acronym Definitions. This table is to be used by the reader as a quick reference guide for acronym definitions.

Acronym	Definition
ARP	Address Resolution Protocol
ASN	Autonomous System Number
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CIDR	Classless Inter-Domain Routing
DSM	Device Support Module
EAL	Evaluation Assurance Level
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
LAN	Local Area Network
NIAP	National Information Assurance Partnership
OSI	Open System Interconnection
P2P	Peer to Peer
PP	Protection Profile
QID	QRadar Identifier
SIM	Security Information Management
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
ST	Security Target
TCP	Transmission Control Protocol
TNC	Trusted Network Computing
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Function
VoIP	Voice over Internet Protocol

Table 1-3: Acronym Definitions

1.1.5 References

[1] Common Criteria for Information Technology Security Evaluation, CCMB-2009-07-004, Version 3.1 Revision 3, July 2009.

[2] U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments Version 1.7

[3] QRadar Administration Guide Release 7.0.0

[4] QRadar Users Guide Release 7.0.0

1.1.6 CC Concepts

The following are CC concepts as used in this document. A Subject is any user of the TOE (account, user, administrative user). An Object (i.e., resource or entity) can be a dataset, volume, command issued by a user, etc. An Operation is any action on a resource (e.g. read, write, create, fetch, update, control, or alter). A Security Attribute is information such as username, groups, profiles, facilities, passwords, etc. that is kept in the security file for the user. An External Entity is anything outside of the TOE that interacts with the TOE.

1.1.7 Protection Profile

This ST claims conformance to the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments Version 1.7 (herein referred to as the IDS System PP). The Protection Profile is conformant to Common Criteria for Information Technology Security Evaluation Part 3 Version 3.1 Revision 3. The IDS System PP states the following:

> *This PP makes a distinction between the System and TOE. The term System is used when the PP is referring to the ID monitoring, analysis, and reaction mechanisms as specified by the IDS security function requirements Class. When the term TOE is used, the PP is referring to the complete IT product that implements all TOE Security Function Requirements necessary to ensure accountability and protection for the ID monitoring, analysis, and reaction capabilities.*

Using the definition of "system" in the IDS System PP, the "authorized System administrator" in the PP has the ability to modify the IDS components of the TOE. "System Administrators" in this ST have the ability to modify the IDS components of the TOE and therefore maps to the term "authorized System administrator" in the IDS System PP. Likewise, the "authorized administrator" in the IDS PP requires access to the IDS (system) data. "Administrator" in this ST has access to the IDS (system) data and therefore maps to the term "authorized administrator" in the IDS System PP.

1.2 TOE Reference

1.2.1 TOE Identification

Q1 Labs QRadar Release 7.0.0

1.3 TOE Overview

Q1 Labs QRadar Release 7.0.0, (herein referred to as QRadar AKA the TOE), is a distributed software only network security management platform that provides situational awareness and compliance support through the combination of flow-based network knowledge, security event correlation, log management and asset-based vulnerability assessment. QRadar collects and processes data including logs from security devices, network devices, applications and databases, network activity data (i.e. flows) from network taps, mirror ports or 3rd party flow sources such as NetFlow, and vulnerability assessment data. The product produces security events by real-time event and flow matching and by comparing the collected data to historical flow-based behavior patterns. The security events are then correlated by the product to produce weighted alerts (i.e. Offenses) which can be viewed in the QRadar Console User Interface as well as sent to users or other solutions via email, syslog, or SNMP trap.

The TOE:

- Provides a customizable interface through which users can view summaries and detailed information about offenses, log and event activity and network activity (flows) occurring on a given network
- Analyzes overall network security, vulnerability states, and network traffic behavior
- Automatically discovers servers and hosts operating on a given network in order to build an asset profile. User identity, vulnerability data and passively learned services information are correlated back to the asset profile.
- Allows users to create, distribute, and manage reports for any data

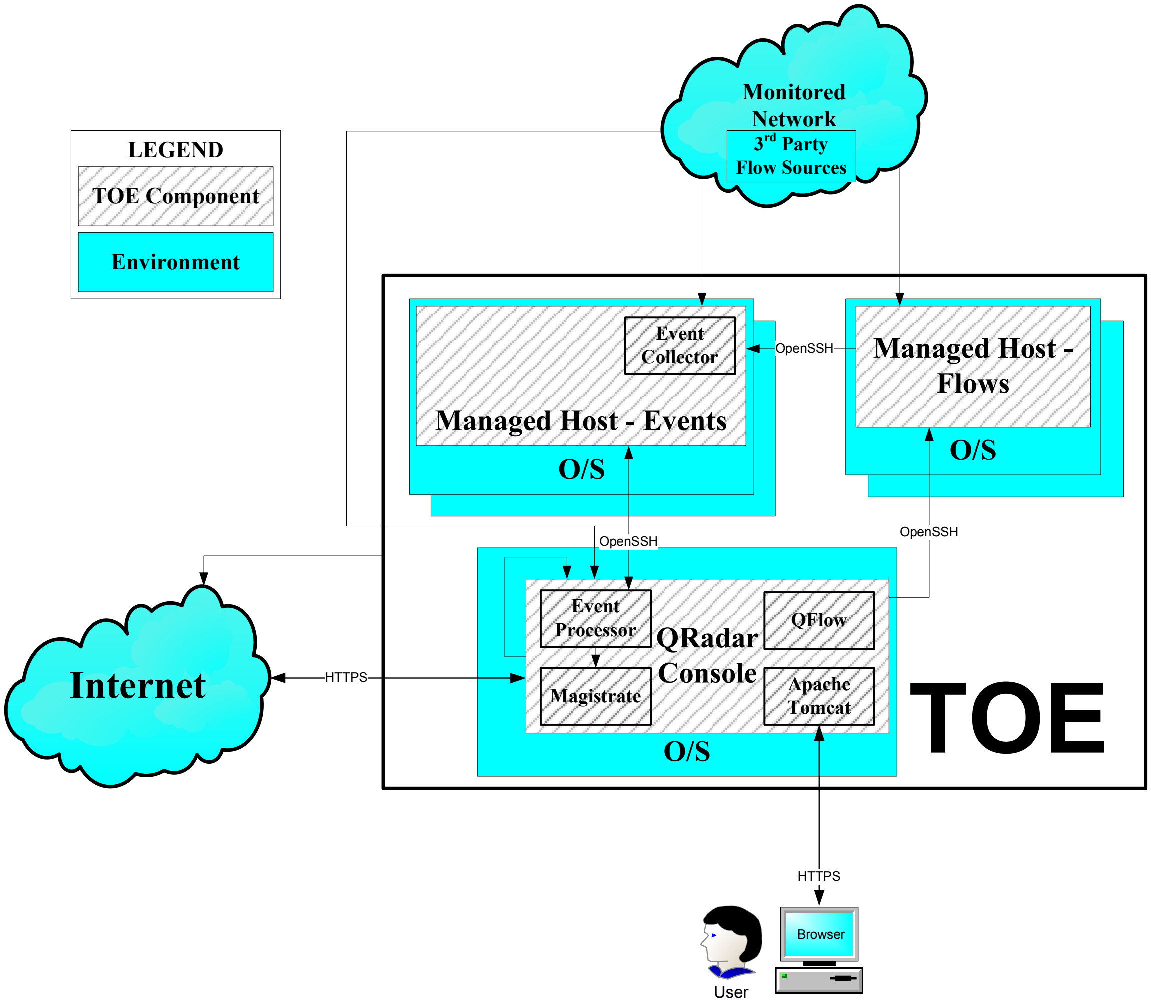


Figure 1 – TOE Boundary

As illustrated in Figure 1, the TOE contains three main subsystems – the QRadar Console, Managed Host - Events, and Managed Host - Flows. The QRadar Console subsystem has the Event Processor and QFlow Collector functionality built in. The Managed Hosts are external to the Console, and can operate on any subset of Console functionality. This is purely for scalability purposes. The evaluated configuration has 4 Managed Hosts: two with Flow functionality that collects flows and two with Event functionality that processes both events and flows. A QRadar deployment is not locked to the evaluated configuration; any number of Managed Hosts can be configured to communicate with a QRadar appliance, and there are several permutations of Managed Host functionality. All subsystems are installed on Operating Systems in the environment (see Section 2.4). Users access the TOE via the QRadar Console (AKA Console). The Magistrate module within the QRadar Console provides real time views, reports, alerts, and in-depth investigation of flows for network traffic, events and log activity and security/policy/compliance Offenses. The QRadar Console deploys configuration changes to the Managed Hosts via a secure path. The Event Collector inside the Managed Host – Events boxes look for the following types of events on the network and downloads them from the network:

- SOAP
- Syslog (TCP)
- Syslog (UDP)
- JDBC/ODBC
- SNMP v1, v2, v3
- Juniper NSM
- Checkpoint Lea
- Cisco SDEE
- Log file protocol (FTP, SCP)
- WindowsDHCPProtocol
- WindowsEventLog
- WindowsEventLogCustom
- WindowsExchangeProtocol
- WindowsIISProtocol
- WindowsTailProtocol
- Sourcefire Defense Center

The Event Collector module within a QRadar appliance, which is considered the scanner component of the TOE, contains the Device Support Module (DSM) which receives or retrieves log and event data and performs the parsing and normalization of logs so that the data can be correlated across all types of devices, and can be easily searched. The

Event Processor module, the analyzer of the TOE, receives the data from the Event Collector. The Event Processor contains QRadar's correlation engine. Correlation and cross-referencing of additional data sources such as asset profile data is performed within the Event Processor to determine offenses committed against the monitored network and assets.

The sensor component of the TOE, QFlow, collects data from devices and various live and recorded feeds, such as network taps, span/mirror ports, as well as 3rd party flow sources (JFlow, NetFlow, Packeteer etc). QFlow then groups related individual packets into a detailed flow record to provided detailed network activity visibility. QFlow contains an advanced application detection engine leveraging both state based classifications to detect applications such as VoIP and P2P, as well as a layer 7 signature based detection module. All flows are accumulated and forwarded to the Event Collector for additional processing. The flows are processed similarly to events in the Event Processor.

The Console subsystem has internal instances of the Event and Flow processes. These processes provide similar functionality to the external Managed Hosts. The Console functionality is primarily to aggregate data taken from one or more Managed Hosts. The Managed Hosts primarily exist for increased processing power and throughput. The QFlow processes send data to Managed Host Event Collectors and the Event Processors send data to the Console Event Processor for aggregation purposes.

There are three types of users within the TOE which are determined by roles - Administrators, System Administrators, and End Users. Each user must be associated with a role, which is created before a user account can be created. Roles determine the privileges that users have in regards to information they have access to, functions they can perform, and what log sources the role has access to. All users must authenticate to the TOE via username and password before they are allowed to perform any functions on the TOE.

End Users in this case are not a specific role, but refer to any role defined in the System that assigns any set of privileges and extended privileges except for Admin. Administrators specifically have complete access to the TOE, which involves having all of the Admin privileges assigned to the role. System Administrators can only configure system data collection standards/protocols and basic QRadar functionality. However, System Administrators cannot edit user accounts, with the exception of changing their own password.

Administrators of the TOE have the ability to perform management functions through the QRadar Console User Interface. This interface gives Administrators with the necessary privileges the ability to manage users, network settings, and TOE settings. End users, on the other hand, have the ability to change their passwords and query reports presented through the QRadar Console User Interface's Dashboard tab. The Dashboard is a customizable view that appears immediately upon user authentication. It allows the privileged subjects 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 tab. End users, similar to administrators, can have privileges assigned to them, allowing them to potentially perform management functions on the TOE.

For more information on management functions on the TOE, see Section 9.1.3.

1.4 TOE Type

The TOE type for Q1 Labs, Inc. QRadar Release 7.0.0 is an Intrusion Detection System. CCEVS defines IDS as the following: “Devices generally deployed on networks or user hosts to monitor traffic and look for evidence of unauthorized intrusions or network attacks.” According to the IDS PP, “An Intrusion Detection System (IDS) monitors an IT System for activity that may inappropriately affect the IT System's assets. An IT System may range from a computer system to a computer network. An IDS System (System) consists of Sensors, Scanners and Analyzers (i.e., IDS components). Sensors and Scanners collect information regarding IT System activity and vulnerabilities, and they forward the collected information to Analyzers. Analyzers perform intrusion analysis and reporting of the collected information.”

2 TOE Description

This ST claims conformance to the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments Version 1.7 (herein referred to as the IDS System PP). The IDS System PP specifies the minimum security requirements for a TOE that is a System. A System is one or more Sensors and/or Scanners, and one or more Analyzers. A System monitors an IT System for activity that may inappropriately affect the IT System's assets, performs analysis on the data it collects, and reacts appropriately. The information collected may be obtained from a variety of sources located on an IT System. Similarly, the response functions may affect one or more targets on the IT System.

The IDS System PP makes a distinction between the System and TOE. The term System is used when the PP is referring to the ID monitoring, analysis, and reaction mechanisms as specified by the IDS security function requirements class. When the term TOE is used, the PP is referring to the complete IT product that implements all TOE Security Function Requirements necessary to ensure accountability and protection for the ID monitoring, analysis, and reaction capabilities.

2.1 Evaluated Subsystems of the TOE

The following table describes the TOE subsystems in the evaluated configuration:

Component	Definition
QRadar Console	The QRadar Console provides the interface for QRadar and is accessed from a standard web browser via https. QRadar supports the following web browsers: • Internet Explorer 7.0 and higher • Mozilla Firefox 3.6 and higher The QRadar Console provides global visibility into real time views, reports, offenses, and in-depth investigation of flows and events. The Magistrate module of the QRadar Console provides views, reports, alerts, and analysis of network traffic and security events. The Magistrate processes the event against the defined custom rules to create an offense. If no custom rules exist, the Magistrate uses the default rules to process the event. An offense is an event that has been processed through QRadar using multiple inputs, individual events, and events combined with analyzed behavior and vulnerabilities. Magistrate prioritizes the offenses and assigns a magnitude value based on several factors, including number of events, severity, relevance, and credibility. Once processed, Magistrate also produces a list for each attacker, which provides administrators with a list

	of attackers for each event. The QRadar Console contains the following two processes internally, and their functionality remains the same. The following subsystems act the same when they are external to the console, and provide additional processing power and throughput to augment the scope of the QRadar deployment.
Managed Host - Events	This Managed Host collects security events from various types of security devices in the network. This Managed Host includes the Event Collector which gathers events from local, remote, and device sources. The Event Collector also bundles all virtually identical events to conserve system usage. The Event Processor correlates security events and logs. Logs that match correlation rules are forwarded to the QRadar Console for additional analysis and possible correlation to an offense. This Managed Host also collects, analyzes and stores data from the Flow Managed Host(s). The Event Processor performs correlation and analysis on the system data (flow data) in order to classify the network activity based on additional characteristics besides applications, such as geography, threatening traffic or other user definable classifications. Additionally, it serves to remove duplicate flows and create aggregate flows.
Managed Host - Flows	This Managed Host collects data from devices and various live and recorded feeds, such as network taps, span/mirror ports (i.e. packet data) as well as 3rd party flow sources such as JFlow, NetFlow, Packeteer flow records etc. This Managed Host contains the QFlow process. The QFlow process groups related individual packets into a flow. A flow starts when the QFlow process detects the first packet with a unique source IP address, destination IP address, source port, and destination port as well as other specific protocol options, which may determine the start of a communication. Each additional packet is evaluated and counts of bytes and packets are added to the statistical counters in the flow record. In addition, QFlow performs layer 7 application analysis on packet data to associate an application id to the flow. This allows QRadar to provide more granular policy monitoring through being able to monitor unsecure or out of policy applications running in an organization. At the end of an interval, a status record of the flow is sent to the Event Collector and statistical counters for the flow are reset. A flow ends when no activity for the flow is seen within the configured period of time. Flow reporting generates records of all the active or expired flows during a specified period of time. QRadar defines these flows as a communication

	session between two pairs of unique IP address/ports that use the same protocol or application.

Table 2-1: Evaluated Components of the TOE

2.2 Components and Applications in the Operational Environment

The following table lists components and applications in the environment that the TOE relies upon in order to function properly:

Component	Definition
Browser	QRadar is accessed from a standard web browser. QRadar supports the following web browsers: • Internet Explorer 7.0 or higher • Mozilla Firefox 3.6 or higher
Monitored Network	QRadar currently only supports IPv4 networks. QRadar cannot build out network objects based on IPv6 addressing. However, QRadar can still monitor, report, and correlate IPv6 data.
Internet	The TOE connects to various third-party company or product websites in order to pull down necessary IDS definition updates. Q1 Labs publishes regular patch updates to their customer's QRadar systems through the auto-update service. (Note: patch updates are disabled in the evaluated configuration.) Q1 Labs also has the ability to send updates of the event and vulnerability mappings.

Table 2-2: Evaluated Components of the Operational Environment

2.3 Excluded from the TOE

The following optional products, components, and/or applications can be integrated with QRadar but are not included in the evaluated configuration. They provide no added security related functionality. They are separated into three categories: not installed, installed but requires a separate license, and installed but not part of the TSF.

2.3.1 Not Installed

These modules are not installed with QRadar and are therefore not included in the TOE boundary.

- **Juniper NSM Console:** The Juniper Networks NSM console passively collects asset information from the network through deployed Juniper IDP sensors. QRadar connects to the Profiler database stored on the NSM server to retrieve these records. The QRadar server must have access to the Profiler database. QRadar supports NSM versions 2007.1r2 to 2007.2r2. This is an extension of the product that only Juniper uses and is therefore excluded from the evaluated configuration.

- **Napatech Interface:** The Naptatech Interface option appears as a configurable packet-based flow source in the QRadar interface if it is installed on your QRadar system. The Napatech Network Adapter provides a next-generation programmable and intelligent network adapter for your network. The use of Napatech cards is only necessary when the rate of traffic is as high as what is supported by this card.

2.3.2 Installed but Requires a Separate License

There are no modules that are installed with QRadar and require a separate license.

2.3.3 Installed But Not Part of the TSF

The following functionality is installed with QRadar, but is not part of the TSF:

- **Command Line Interface (CLI) –** The CLI is used by the root user to directly access the database within the Event Processor via the QRadar Console. This interface is excluded because the root user is not included in the evaluated configuration. The information in the database is viewed as reports by remote users logging in to the QRadar Console User Interface.

- **RADIUS, TACACS, LDAP, AD –** These third-party authentication mechanisms are scoped out of the TOE because the TOE contains this functionality within the primary TSF. Adding these additional functionalities to the evaluation provides no added benefit or functionality.

2.4 Physical Boundary

The Target of Evaluation (TOE) is a distributed, software-only TOE. QRadar is available installed in all-in-one 'Appliance' products or may be installed by the end-user on a suitable hardware platform. The TOE requires dedicated hardware.

QRadar supports the following hardware and OS platforms:

- Hardware platform: QRadar requires an Intel PC Platform for each of the QRadar subsystems. The same basic configuration is used for each subsystem in the QRadar system. To maximize throughput, a dedicated server for each subsystem is recommended.

- OS platform: QRadar runs on CentOS release 5.4 for all product subsystems in the evaluated configuration. The product is also supported and tested to run on Red Hat Enterprise Linux Server 5.3 (Tikanga). The TOE is not tied to any given release of any operating system, but the OS used in the evaluated configuration is CentOS release 5.4.

QRadar requires the following software packages to be installed to utilize the TOE functionality:

- Web browser: Internet Explorer 7.0 or higher or Mozilla FireFox 3.6 or higher are the supported web browsers.

- Java Runtime Environment (JRE) v6.16 or higher

The following table lists the minimum hardware requirements for each subsystem of the TOE. The table shows that multiple hardware boxes are required for QRadar to be fully functional.

Console	Managed Host - Events	Managed Host - Flows
2x 2.80 GHz Intel Xeon Processor or equivalent	2x 2.80 GHz Intel Xeon Processor or equivalent	2x 2.80 GHz Intel Xeon Processor or equivalent
8 GB RAM	8 GB RAM	6 GB RAM
200 MB installation	50 MB installation	50 MB installation
600 GB data storage (RAID recommended)	140 GB data storage (RAID recommended)	140 GB data storage
4x 10/100/1000 network interfaces	4x 10/100/1000 network interfaces	4x 10/100/1000 network interfaces

Table 2-3: Minimum Hardware Requirements for the TOE

Note that these requirements reflect the capability of the TOE to process events from up to 1,000 distinct network sources and process flows with a combined throughput of up to 1 Gbps.

2.5 Logical Boundary

The logical boundary of the TOE is described in the terms of the security functionalities that the TOE provides to the systems that utilize this product for information flow control.

The logical boundary of the TOE is broken down into six security classes: Security Audit, Identification and Authentication, Security Management, Encrypted Communications, Protection of the TSF, and Intrusion Detection System. Listed below are the security functions with a listing of the capabilities associated with them.

2.5.1 Security Audit

The TOE creates syslog audit events for actions taken within QRadar, which are populated with reliable timestamps provided by the TOE, event types, identity, outcome, and additional information for each type of audit event. The identity of the user changing the TOE is also reflected in the events. The TOE allows a role with System Administrator privileges to read audit information from the event, with sorting options. All other users are not authorized to view the audit information. Users without these privileges are denied access to the audit events. Audit information can also be displayed as reports.

The TOE is able to modify inclusion parameters for audit events, effectively narrowing or broadening the scope of what is recorded. Authorized or Unauthorized users are not able to delete audit events, and all modifications are detected by the TOE. When audit storage is filled to capacity, the most recent events are preserved while the oldest are deleted. An alarm is sent to the configured user in the case of this event.

More information about the auditing process can be found in Section 9.1.1.

2.5.2 Identification & Authentication

The TOE identifies and authenticates users via their usernames and passwords. The TOE requires all users to authenticate through a browser to Apache Tomcat on the QRadar Console before performing any administrative functions on the TOE. No actions on the TOE can be performed by a user until he or she is identified and authenticated to the TOE. Once authenticated, all users are assigned a role, which is one of the security attributes maintained by the TOE. The role determines what actions the user is authorized to perform on the TOE. The TOE locks out users for a configurable period of time after a configurable number of failed access attempts. Similarly, the product provides methods of updating patch and signature (event and vulnerability mappings) information coming from the Q1 servers. In the evaluated configuration, the TOE will not download and apply patch updates without an Administrator action.

2.5.3 Encrypted Communications

Remote users establish a session with the TOE using a web-based HTTPS session. This secured path is used for user authentication, management and operations of the TOE by authorized users. The TOE generates cryptographic keys to support the use of OpenSSH during communication with remote users and between TOE subsystems.

2.5.4 Protection of the TSF

Administrators of the TOE ensure that all connections between physically separate parts of the TOE (i.e. trusted remote product) are secured using OpenSSH. All data transmitted between TOE subsystems is protected from unauthorized disclosure and modification during transmission. This includes all system data that is passed between TOE subsystems once a scanning session is completed and the data is made. The TOE uses secure hashing to verify the integrity of transmitted data, including detection of any unauthorized modifications of the data.

2.5.5 Security Management

All management functions and user operations are performed through the QRadar Console User Interface. The TOE has three roles: Administrators, System Administrators, and End Users. Administrators have all privileges, which include the managing of user accounts and configuring system data collection standards/protocols. System Administrators only have the privileges to configure system data collection standards/protocols, basic QRadar functionality, and to change their own account passwords. Only Administrators and System Administrators roles can create, modify, and delete rules that modify the behavior of the IDS functionality of the TOE.

End User roles do not have Admin privileges. End users have the ability to modify their own account passwords and query pre-defined reports. End users may be assigned additional privileges that enable them to perform more operations on the TOE, including Reports, Offense Manager with Customized Rule, Offense Manager, and other privileges as defined by an administrator. For more detailed information on specific privileges users and administrators possess, refer to Section 9.1.3.

2.5.6 Intrusion Detection System

The TOE is an Intrusion Detection System which collects various sets of information from the targeted resources, including but not limited to start-up, shutdown, and network traffic. The collected traffic is distributed into groups by the TOE for analysis and reporting purposes. Users are able to view this data based on their role. For more information on this data, see Tables 7-3 and 7-4. The TOE analyzes this data to establish whether a correlation exists with behavior and events. Each analytical result records the date/time of the result, the type of result, the identity of the data source, and the overall analysis of the results. All system data is stored by the TOE and is protected from unauthorized deletion and modification. Once the storage capacity is reached, the TOE ensures that the most recent data is maintained. The TOE overwrites the oldest stored data and sends an alarm to the configured user when this occurs. After the analysis has occurred and the TOE determines that an intrusion has been detected, the system sends an alarm to the configured user.

2.6 TOE Self Protection

Users are only able to access the Console through the User Interface which requires them to first be identified and authenticated to the TOE. All of the other interactions with any of the other systems must be mediated by the Console. Similarly, databases are replicated between components so a database could not be changed on a managed host unless a root-level system account did so. Flat files on the OS are stored in root context, so a root-level system account would be required. The root account on the system is only used for setup and troubleshooting and should not be used for general TOE operations.

The following information addresses the issue of domain separation between the TOE and the Operational Environment. The TOE is a software product that is running upon a hardware platform. The operational environment in this case would be comprised of the operating system on which the TOE is installed, and the JRE and web browser that are used on the remote client to access the TOE. The operating system provides kernel-level operations and control and file-system level protection. Local users of the QRadar appliance must also be considered users of the operational environment’s OS (CentOS), because the TOE does not share any authentication credentials with the operational environment. In the evaluated configuration local users are not scoped into the TOE, because the only user interface within the TOE is the remote user via the web browser to Console (Web GUI). This means that the TOE hosts a web server that users can connect to over the local network within the evaluated configuration. The TOE relies on the web browser and the JRE to provide users access to the TOE’s Console interface, and provide a trusted path between the remote user and the TOE. This requires the web browser, the JRE, and the TOE’s web server to establish an encrypted session that will protect the data that traverses the path from modification and disclosure, before any other data is transferred over this path.

No external connections to data stores exist, meaning that the only way to interact with said data stores is through the TOE. They aren’t exposed to the network. Each major data store has its own process component that mediates the communications between the data store and what component is trying to access it. Users are unable to interact directly with collected IDS data to obfuscate network activity.

In terms of non-bypassability, the TOE maintains a strict data flow for authentication, authorization, and viewing TOE data. In the evaluated configuration, the only user interface to the TOE is from the user's web browser to the Console. A web server is in charge of validating authentication requests, and no actions are available to TOE users until they have authenticated. During authentication the web browser will generate a unique value that will identify that session. This unique value is stored by the TOE's web server locally to associate future requests with that session and is also placed within a cookie that is stored within the web browser. This allows the TOE to maintain multiple user sessions simultaneously. Once a user is authenticated, the actions they are allowed to do, based on their role, are available to be performed. Each request made by a user via the web browser is sent with the session cookie which the TOE utilizes to associate with the user's session and thus their role. This information is then used to determine if the action is authorized to be performed. If authorized, the TOE will take action on the request. If the user is not authorized, the TOE will reject the request and inform the user they are not authorized.

In addition, actions that a user isn't allowed to perform are not even displayed to the user's web browser by the TOE. However, if a user attempts to URL hack a Console page to get access to functions they are not allowed, the Console also contains the functionality to determine that said function is outside of the scope of their role and therefore will not be authorized. The only way to access TOE data through the TOE itself is through this Console. The evaluated configuration has scoped out the CLI component, which connects directly to the System data storage. This CLI component requires that a user is a root admin on the QRadar box, which has been determined to be an unsecure and non-standard configuration based upon the security objectives defined within the ST and PP. In terms of flow data potentially bypassing the TOE functionality, all event logs formulated by third-party devices are sent directly to the TOE, and the TOE processes the data received accordingly.

Users derive the ability to interact with the TOE through their assigned role. Administrators have the ability to create user accounts and roles. Roles are defined as a bundle of privileges and log sources. Therefore, assigning a user to a role is in essence assigning the user a list of permissions and log sources. Each of the primary functionalities in the TOE has a role associated with it, with extended privileges allowing further granular control. The interface operates on a tab system; tabs will become available to users according to their privileges defined by their role. A user cannot even attempt to perform an action that they aren't privileged to perform, as the tabs and by extension the options themselves are not visible.

Trusted channels are used between every TOE component and through the connections to the Internet. Trusted paths are established by the TOE whenever a user connects to the TOE remotely via a web browser. No trusted channel is used between the TOE and the Monitored Network. OpenSSH is used for internal TOE communications. The various TOE components are able to validate the identity of each other to preserve the integrity of

TOE communications. HTTPS (OpenSSL) is used for external communications to the Internet and the web browser connection. AES and RSA encryption are used with 256 and 1024-bit key sizes, respectively.

3 Conformance Claims

3.1 CC Version

This ST is compliant with *Common Criteria for Information Technology Security Evaluation*, CCMB-2009-07-004, Version 3.1 Revision 3, July 2009.

3.2 CC Part 2 Conformance Claims

The ST and Target of Evaluation (TOE) are Part 2 conformant to the US Government Protection Profile Intrusion Detection System System for Basic Robustness Environments v.1.7. Additionally, the ST and TOE are Part 2 conformant for EAL3 for added SFRs outside the IDS System PP. This includes all applicable NIAP and International interpretations through 28 October 2009.

3.3 CC Part 3 Conformance Claims

The ST and TOE are Part 3 conformant to the US Government Protection Profile Intrusion Detection System System for Basic Robustness Environments v.1.7, with all hierarchical SARs consistent with EAL3. This includes all applicable NIAP and International interpretations through 28 October 2009.

3.4 PP Claims

This ST claims demonstrable conformance to US Government Protection Profile Intrusion Detection System System for Basic Robustness Environments v.1.7. The Protection Profile is conformant to Common Criteria for Information Technology Security Evaluation Part 3 Version 3.1 Revision 3.

3.5 Package Claims

In addition to the US Government Protection Profile Intrusion Detection System System for Basic Robustness Environments v.1.7 being met by this TOE, hierarchical SARs consistent with EAL3 have been claimed. Therefore, this TOE claims an assurance package for EAL3.

3.6 Package Name Conformant or Package Name Augmented

This ST and TOE is conformant to EAL3 package claims augmented with ALC_FLR.2.

3.7 Conformance Claim Rationale

The ST and TOE are conformant to the US Government Protection Profile Intrusion Detection System System for Basic Robustness Environments v.1.7. All SFRs stated in this ST are either conformant to CC Part 2 or the IDS System PP. All SFRs in the IDS System PP have been claimed in this ST. According to the IDS System PP, "Intrusion Detection System System Protection Profile-conformant products support the ability that monitor (both real-time and statically) an IT System for activity that may inappropriately affect the IT System's assets and react appropriately. Intrusion Detection System System Protection Profile-conformant products also provide the ability to protect themselves and their associated data from unauthorized access or modification and ensure accountability for authorized actions. The Intrusion Detection System System Protection Profile was constructed to provide a target and metric for the development of Systems. This ST identifies security functions and assurances that represent the lowest common set of requirements that should be addressed by a useful IDS System." The product under evaluation is being evaluated at a level of EAL3, which is higher than the "lowest common set of requirements that should be addressed by a useful IDS System." Since the IDS System PP has previously been evaluated and this TOE exceeds a minimum standard of demonstrable conformance to the IDS PP, this TOE accurately claims conformance to the IDS System PP.

4 Security Problem Definition

4.1 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 for all the threats is unsophisticated.

4.1.1 TOE Threats

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

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

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

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

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

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

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

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

T.EAVESDROPPING A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.

4.1.2 IT System Threats

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

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

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

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

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

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

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

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

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

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

4.2 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 the IDS System PP.

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

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

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

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

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

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

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

4.3 Assumptions

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

4.3.1 Intended Usage Assumptions

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

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

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

4.3.2 Personnel Assumptions

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

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

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

4.3.3 Physical Assumptions

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

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

5 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.

5.1 IT Security Objectives

The following are the TOE security objectives:

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

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

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

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

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

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

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

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

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

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

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

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

O.EAVESDROPPING The TOE will encrypt TSF data that traverses the network to prevent malicious users from gaining unauthorized access to TOE data.

5.2 Security Objectives for the operational environment of the TOE

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

OE.AUDIT_PROTECTION The IT Environment will provide the capability to protect audit information.

OE.AUDIT_SORT The IT Environment will provide the capability to sort the audit information.

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

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

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

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

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

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

OE.KEYDESTRUCT The Operational Environment of the TOE is in charge of destroying cryptographic keys when they are no longer necessary.

6 Extended Security Functional and Assurance Requirements

6.1 Extended Security Functional Requirements for the TOE

There are no extended Security Functional Requirements for this ST outside of the requirements that the Protection Profile includes.

6.2 Extended Security Assurance Requirements

There are no extended Security Assurance Requirements in this ST.

7 Security Functional Requirements

7.1 Security Functional Requirements for the TOE from the IDS System PP

This section defines the functional requirements for the TOE, as defined in the IDS System PP. Functional requirements in the IDS System PP were drawn from Part 2 of the CC. These requirements are relevant to supporting the secure operation of the TOE. Functional requirements pertaining to the System collection, analysis, and reaction mechanisms were invented and are identified by the short name IDS.

The functional security requirements for the IDS System PP consist of the following components, summarized in the following table.

Security Function	Security Functional Components
Security Audit (FAU)	FAU_GEN.1 Audit data generation
	FAU_SAR.1 Audit review
	FAU_SAR.2 Restricted audit review
	FAU_SAR.3 Selectable audit review
	FAU_SEL.1 Selective audit
	FAU_STG.2 Guarantees of audit data availability
	FAU_STG.4 Prevention of Data Loss
Identification and Authentication (FIA)	FIA_UAU.1 Timing of authentication
	FIA_ATD.1 User attribute definition
	FIA_UID.1 Timing of identification
	FIA_AFL.1 Authentication failure handling
Security Management (FMT)	FMT_MOF.1 Management of security functions behavior
	FMT_MTD.1 Management of TSF data
	FMT_SMR.1 Security roles
Protection of the TSF (FPT)	FPT_STM.1 Reliable time stamps
	FPT_ITA.1 Inter-TSF availability within a defined availability metric
	FPT_ITC.1 Inter-TSF confidentiality during transmission
	FPT_ITI.1 Inter-TSF detection of modification
Intrusion Detection System (IDS)	IDS_SDC.1 System Data Collection
	IDS_ANL.1 Analyzer analysis
	IDS_RCT.1 Analyzer react
	IDS_RDR.1 Restricted Data Review
	IDS_STG.1 Guarantee of System Data Availability
	IDS_STG.2 Prevention of System data loss

Table 7-1: Security Functional Requirements for the TOE from the IDS PP

7.1.1 Class FAU: Security Audit

7.1.1.1 FAU_GEN.1 Audit data generation

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

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

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

c) **Access to the System and access to the TOE and System data.**

Application Note: *The auditable events for the basic level of auditing are included in Table 7-2 Auditable Events below.*

Component	Event	Additional Details
FAU_GEN.1	Start-up and shutdown of audit functions	None
FAU_GEN.1	Access to System	None
FAU_GEN.1	Access to the TOE and System data	Object IDS, Requested access
FAU_SAR.1	Reading of information from the audit records	None
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	None
FAU_SEL.1	All modifications to the selection of audit events that occur while the audit collection functions are operating	None
FIA_UAU. 1	All use of the authentication mechanism	User identity, location
FIA_UID.1	All use of the user identification mechanism	User identity, location
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	None
FMT_MTD.1	All modifications to the values of TSF data	None
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity
FMT_MTD.1	All modifications to the values of TSF data by users and administrators	User identity
FMT_SMF.1	All use of Security and IDS management functions	User identity
FTP_TRP.1	Initiation of Trusted Path and all management of the TOE and its data	User identity

Table 7-2: Auditable Events

Application Note: *The IDS_SDC and IDS_ANL requirements in the IDS System PP address the recording of results from IDS scanning, sensing, and analyzing tasks (i.e., System data)*

Application Note: *The term audit record is synonymous with audit log.*

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

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

b) **For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST,** the additional information specified in the **Details** column of the table above.

7.1.1.2 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [***users with the System Administrator privilege***] with the capability to read [***all audit information]*** from the audit records.

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

Application Note: The term audit record is synonymous with audit event.

7.1.1.3 FAU_SAR.2 Restricted audit review

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

Application Note: The term audit record is synonymous with audit event.

7.1.1.4 FAU_SAR.3 Selectable Audit Review

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

7.1.1.5 FAU_SEL.1 Selective audit

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

a) <u>event type;</u>

b) [***None***]

7.1.1.6 FAU_STG.2 Guarantees of audit data availability

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

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

FAU_STG.2.3 The TSF shall ensure that [***the last 30 days of the***] audit records will be maintained when the following conditions occur: [***audit storage exhaustion]***

Application Note: *The term audit record is synonymous with audit event.*

7.1.1.7 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall [**overwrite the oldest stored audit records**] and send an alarm if the audit trail is full.

Application Note: *The act of sending an alarm is represented by sending an email to the configured user.*

Application Note: *The term audit record is synonymous with audit event.*

7.1.2 Class FIA: Identification and Authentication

7.1.2.1 FIA_UAU.1 Timing of authentication

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

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

7.1.2.2 FIA_AFL.1 Authentication failure handling

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

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **prevent**

the offending external IT product from successfully authenticating until an authorised administrator takes some action to make authentication possible for the external IT product in question.

Application Note: *The settable, non zero number of authentication attempts is 1. The values involved in the authentication failure system are able to be configured by an Administrator.*

Application Note: *The TOE uses SSH (OpenSSH) to receive IDS definition updates from Q1 Labs.*

7.1.2.3 FIA_ATD.1 User attribute definition

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

a) User identity;

b) Authentication data;

c) Authorizations; and

d) [***Assigned role, CIDR address ranges, log sources, and log source groups].***

Application Note: *A User can be an Administrator, a System Administrator, or an End User. A User is considered a System Administrator if he has the System and Views Administrator extended privileges, an Administrator if he has all the Admin extended privileges, and an End User if he has no Admin privileges.*

Application Note: *At a minimum, there must be sufficient user information for identification and authentication purposes. That information includes maintaining any authorisations a user may possess.*

7.1.2.4 FIA_UID.1 Timing of identification

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

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

7.1.3 Class FMT: Security Management

7.1.3.1 FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behavior of the functions of **System data collection, analysis and reaction** to authorized System administrators.

Application Note: *End Users can be given access to modify analytic rules, but they must be given this privilege by an Administrator. Once the End user has this privilege, he or she is then considered an authorized system administrator.*

7.1.3.2 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to query **and add System and audit data, and shall restrict the ability to query and modify all other TOE data** to [***roles with assigned privileges as defined in Tables 7-6, 7-7, and 7-8***].

Application Note: *Users are separated into administrator and non-administrator roles. Within each role, there are privileges assigned that determine which operations can be performed on which sets of TOE data.*

7.1.3.3 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the **following *roles*: authorized administrator, authorized System Administrators, and** [***End User***].

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

Application Note: *The End User role can have one or more of the following privileges: Offenses, Log Activity, Assets, Resolution, Network Activity, Reports, and IP Right Click Menu Extensions. These privileges are assigned by an Administrator with the Administrator Manager extended privilege.*

Application Note: *The Administrator role can have one or more of the following extended privileges: Administrator Manager, Remote Networks and Services Configuration, and System Administrator.*

Application Note: *Authorized Administrator is synonymous with Administrator. Authorized System Administrator is synonymous with System Administrator.*

7.1.4 Class FPT Protection of the TOE Security Functions

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

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

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

Application Note: *"Immediately" in this case implies that the data is available without any user actions needed.*

7.1.4.2 FPT_ITC.1 Inter-TSF confidentiality during transmission

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

Application Note: *The TOE uses the SSH protocol to protect the confidentiality of all TSF data that is transmitted between the TSF and any remote trusted IT products (i.e. TOE subsystems).*

7.1.4.3 FPT_ITI.1 Inter-TSF detection of modification

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [***immediately upon modifications detected by HMAC-MD5 secure hashing***].

Application Note: *"Immediately" in this case implies that the data is available without any user actions needed.*

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [***drop the packet and request the packet to be retransmitted***] if modifications are detected.

7.1.4.4 FPT_STM.1 Reliable time stamps

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

Application Note: FPT_STM.1 is included in the IDS System PP; however, this contradicts OE.TIME: "The IT Environment will provide reliable timestamps to the TOE.", which is also part of the IDS System PP. This ST will treat FPT_STM.1 as an IT Environment SFR.

7.1.5 Class IDS: Intrusion Detection System Component Requirements

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

7.1.5.1 IDS_SDC.1 System Data Collection (EXT)

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

a) [**Start-up and shutdown, identification and authentication events, data accesses, service requests, network traffic, security configuration changes, data introduction, detected malicious code, access control configuration, service configuration, authentication configuration., accountability policy configuration, detected known vulnerabilities**]; and

b) [***The additional System data as listed in Table 7-3 below***]**. (EXT)**

Event	Details
Network traffic	Protocol, application, content, source port, destination port, source address, destination address, TCP flags
Host profiles	Open Ports, Services, IP Addresses

Table 7-3: System data

Application Note: *Information from the targeted IT System Resource is distributed into the following groups:*

- *Recon - Events relating to scanning and other techniques used to identify network resources, for example, network or host port scans.*
- *DOS - Events relating to Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks against services or hosts, for example, brute force network DoS attacks.*
- *Authentication - Events relating to authentication controls, group, or privilege change, for example, log in or log out.*
- *Access - Events resulting from an attempt to access network resources, for example, firewall accept or deny.*
- *Exploit - Events relating to application exploits and buffer overflow attempts, for example, buffer overflow or web application exploits.*
- *Malware - Events relating to viruses, trojans, back door attacks, or other forms of hostile software. This may include a virus, trojan, malicious software, or spyware.*
- *Suspicious Activity - The nature of the threat is unknown but behavior is suspicious including protocol anomalies that potentially indicate evasive techniques, for example, packet fragmentation or known IDS evasion techniques.*
- *System - Events related to system changes, software installation, or status messages.*
- *Policy - Events regarding corporate policy violations or misuse.*
- *CRE (Custom Rule) - Events generated from an offense or event rule. For more information on creating custom rules, see the QRadar Administration Guide.*
- *Potential Exploit - Events relating to potential application exploits and buffer overflow attempts.*

- *SIM Audit - Events relating to user interaction with the Console and QRadar Administration Console.*
- *VIS Host Discover - Events relating to the host, ports, or vulnerabilities that the VIS module discovers.*
- *Application – Events relating to application activity.*

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

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

b) The additional information specified in the Details column of Table 7-4 below. (EXT)

Component	Event	Details
IDS_SDC.1	Start-up and shutdown	**none**
IDS_SDC.1	Identification and authentication events	**User identity, location, source address, destination address**
IDS_SDC.1	Data accesses	**Object IDS, requested access, source address, destination address**
IDS_SDC.1	Service Requests	**Specific service, source address, destination address**
IDS_SDC.1	Network Traffic	**Protocol, source address, destination address**
IDS_SDC.1	Security configuration changes	**Source address, destination address**
IDS_SDC.1	Data introduction	**Object IDS, location of object, source address, destination address**
IDS_SDC.1	Start-up and shutdown of audit functions	**none**
IDS_SDC.1	Detected malicious code	**Location, identification of code**
IDS_SDC.1	Access control configuration	**Location, access settings**
IDS_SDC.1	Service configuration	**Service identification (name or port), interface, protocols**
IDS_SDC.1	Authentication configuration	**Account names for cracked passwords, account policy parameters**
IDS_SDC.1	Accountability policy configuration	**Accountability policy configuration parameters**
IDS_SDC.1	Detected known vulnerabilities	**Identification of the known vulnerability**

Table 7-4: System Events

Application Note: *In the case where a Sensor is collecting host-based events, for the identification and authentication event, the source address could be a subject IDS on a local machine and the* *destination is defined by default. For the data access and data introduction events, the source address could be filename and the destination address may be target location for the file.*

7.1.5.2 IDS_ANL.1 Analyzer analysis (EXT)

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

a) [**statistical, signature, integrity**]; and
b) [***no other analytical functions***]. **(EXT)**

Application Note: *Statistical analysis involves identifying deviations from normal patterns of behavior. For example, it may involve mean frequencies and measures of variability to identify abnormal usage. Signature analysis involves the use of patterns corresponding to known attacks or misuses of a System. For example, patterns of System settings and user activity can be compared against a database of known attacks. Integrity analysis involves comparing System settings or user activity at some point in time with those of another point in time to detect differences.*

Application Note: *In the evaluated configuration, behavioral and event correlation map to statistical, signature, and integrity analysis.*

Application Note: *The term IDS data is synonymous with system data.*

IDS_ANL.1.2 **The System shall record within each analytical result at least the following information:**

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

b) [***analysis results***]. **(EXT)**

Application Note: *The following information is stored if it is available:*

- *Source or Destination IP*
- *Category*
- *Destination Asset Name*
- *Destination IP*
- *Destination Port*
- *Log Source*
- *Log Source Group*

- *Source Asset Name*
- *Source IP*
- *Event Name*
- *Associated With Offense*
- *Credibility*
- *Destination MAC*
- *Destination Network*
- *Direction*
- *Duration*
- *End Time*
- *Event Count*
- *Event Is Unparsed*
- *High Level Category*
- *IPv6 Destination*
- *IPv6 Source*
- *Is CRE Event*
- *Log Source Time*
- *Log Source Type*
- *Magnitude*
- *Matched Custom Rule*
- *Payload*
- *Post NAT Destination IP*
- *Post NAT Destination Port*
- *Post NAT Source IP*
- *Post NAT Source Port*
- *Pre NAT Destination IP*
- *Pre NAT Destination Port*
- *Pre NAT Source IP*
- *Pre NAT Source Port*
- *Protocol*
- *Relevance*
- *Severity*
- *Source MAC*
- *Source Network*
- *Source Port*
- *Source or Destination Network*
- *Source or Destination Port*
- *Start Time*
- *Username*
- *Any user-defined field*

Application Note: *The analytical conclusions drawn by the analyser should both describe the conclusion and identify the information used to reach the conclusion.*

7.1.5.3 IDS_RCT.1 Analyzer react (EXT)

IDS_RCT.1.1 **The System shall send an alarm to** [***one or more of the following: QRadar Console User Interface, to the QRadar system log, a notification via email, or to a remote machine via SNMP trap***] **and take** [***no other action***] **when an intrusion is detected. (EXT)**

Application Note: *The term "remote machine" refers to any IP address that is specified in the rule for SNMP notifications.*

Application Note: *The email notification can be configured to specify which email address(es) are sent the notification.*

7.1.5.4 IDS_RDR.1 Restricted Data Review (EXT)

IDS_RDR.1.1 **The System shall provide** [***each user***] **with the capability to read** [***all system data defined by their role and allowed devices by group or range]*** **from the System data. (EXT)**

Application Note: *The specific System data a user is able to read is defined by their role and allowed devices by group, range or type.*

IDS_RDR.1.2 **The System shall provide the System data in a manner suitable for the user to interpret the information. (EXT)**

IDS_RDR.1.3 **The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access. (EXT)**

7.1.5.5 IDS_STG.1 Guarantee of System Data Availability (EXT)

IDS_STG.1.1 **The System shall protect the stored System data from unauthorized deletion. (EXT)**

IDS_ STG.1.2 **The System shall protect the stored System data from modification. (EXT)**

Application Note: *Authorized deletion of data is not considered a modification of System data in this context. This* *requirement applies to the actual content of the System data, which is protected from any modifications.*

IDS_STG.1.3 **The System shall ensure that [*the most recent*] System data will be maintained when the following conditions occur:** [**System data storage exhaustion**]. **(EXT)**

Application Note: *When the TOE's internal database detects the disk partition is running out of space (< 15% disk free), it will begin compressing data (loss-lessly). It will stop compressing when >= 18% disk partition is free. If 18% of the disk partition cannot be freed, old records (events / flows) will be deleted starting with the oldest records until >=18% of the disk partition is freed. When the TOE itself detects that it has >95% disk partition usage (system data storage exhaustion) the system will shut down. The TOE will recover automatically if compression and deletion of records results in >= 18% of the disk partition being freed.*

7.1.5.6 IDS_STG.2 Prevention of System data loss (EXT)

IDS_STG.2.1 **The System shall** [**overwrite the oldest stored System data**] **and send an alarm if the storage capacity has been reached. (EXT)**

Application Note: *The act of sending an alarm is represented in IDS_RCT.1.*

7.2 Additional Security Functional Requirements for the TOE

The following table provides a summary of additional Security Functional Requirements implemented by the TOE that go above and beyond those provided by the IDS System PP. These SFRs are pulled from CC Part 2.

Security Function	Security Functional Components
Cryptographic Support (FCS)	FCS_CKM.1 Cryptographic key generation
	FCS_COP.1 Cryptographic operation
Identification and Authentication (FIA)	FIA_AFL.1(1) Authentication Failure handling
Security Management (FMT)	FMT_MTD.1(1) Management of TSF data
	FMT_MTD.1(2) Management of TSF data
	FMT_MTD.1(3) Management of TSF data
	FMT_MTD.1(4) Management of TSF data
	FMT_SMF.1 Specification of management functions

Security Function	Security Functional Components
Trusted Path/Channel (FTP)	FTP_TRP.1 Trusted Path

Table 7-5: Additional Security Functional Requirements for the TOE

7.2.1 Cryptographic Support (FCS)

The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

7.2.1.1 FCS_CKM.1 Cryptographic Key Generation

Hierarchical to: No other components.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [***RSA***] and specified cryptographic key sizes [***1024-bits***] that meet the following: [***RFC 4432***].

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

Application Note: This SFR supports key management for OpenSSH and OpenSSL.

7.2.1.2 FCS_COP.1 Cryptographic Operation

Hierarchical to: No other components.

FCS_COP.1.1 The TSF shall perform [***encryption and decryption***] in accordance with a specified cryptographic algorithm [***AES in CBC mode***] and cryptographic key sizes [***256 -bits***] that meet the following: [***RFC 3602***].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

Application Note: This SFR supports encryption and decryption for OpenSSH and OpenSSL.

7.2.2 Class FIA: Identification and Authentication

7.2.2.1 FIA_AFL.1 (1) Authentication Failure Handling

Hierarchical to: No other components.

FIA_AFL.1.1 (1) The TSF shall detect when an administrator configurable positive integer within [***5***] unsuccessful authentication attempts occur related to [***user authentication*****].**

FIA_AFL.1.2 (1) When the defined number of unsuccessful authentication attempts has been [**met**], the TSF shall [***lockout the host from where the login attempt was made for 30 minutes***].

Dependencies: FIA_UAU.1 Timing of authentication

Application Note: The number of unsuccessful attempts (default 5), the time period in which the attempts occur (default 10 minutes) and the amount of time the host from where the login attempt was made is locked out (default 30 minutes) are all configurable by the Administrator.

7.2.3 Class FMT: Security Management

7.2.3.1 FMT_MTD.1 (1) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 (1) The TSF shall restrict the ability to ***[Perform operations listed in Table 7-6 below]*** the [***TSF data listed in Table 7-6 below]*** to [***Administrators and System Administrators***].

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

Operations selection and assignment	TSF data assignment	Role
Query, Modify, Delete	User Data: • TSF data required to manage Identification and Authentication for Users as defined by FIA_ATD.1 except for the password component of their authentication data.	Administrator

	System Data: • Configure collection of data from IDS_SDC.1. • Reporting interface to all System data • Rules applied to system data from which alerts (IDS_RCT.1) are generated, including email notification and logging. • Threshold level and email notice location for System data storage required for IDS_STG.1.1. • Define the data to be collected by the QFlow Collectors, as specified in IDS_SDC.1	Administrator and System Administrator
Query	User Data: • Audit event data	Administrator
	System Data: • All System data • Alerts generated by the TSF	Administrator and System Administrator

Table 7-6: Operations Performed by Administrators and System Administrators

7.2.3.2 FMT_MTD.1 (2) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 (2) The TSF shall restrict the ability to **[*Perform operations listed in Table 7-7 below*]** the [***TSF data listed in Table 7-7 below for the data related to the CIDR ranges, devices, and device groups specified by the Administrator for each user*]** to [***the Privilege Assignment listed in Table 7-7 below***].

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

Operations Selection and Assignment	TSF Data Assignment	Privilege Assignment
Query	Pre-defined Dashboard Report	Users
View	Audit Event data	Users with System Administrator privilege
Query, Modify, Delete, Create	Reporting interface to System data	Users with Reports privileges
Query, Modify, Delete, Create	Configuration for rules applied to the system data from which Alerts (IDS_RCT.1) are generated, includes email notification and logging.	Users with Offense Manager with Customized Rule privileges
Query, Modify, Delete, Create	Configuration for the rules applied to the system data (flow	Users with Offense Manager privileges

	data) from which alerts (IDS_RCT.1) are generated, includes email notification and logging.	
Query	System data (Flow data)	
Query, Create, Modify, Delete	Rules applied to system data from which alerts (IDS_RCT.1) are generated	Users with Offense Rules or Event Rules privileges

Table 7-7: Operations Performed by Privileged Users

7.2.3.3 FMT_MTD.1 (3) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1(3) The TSF shall restrict the ability to **[*query*]** the [***System data for a report or an alert]*** to [***users***] with [***Report sharing privileges (for reports) and Offense Manager sharing privileges (for alerts)***].

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

Application Note: The devices that a user can perform management functions against are determined by the following attributes for that user: CIDR address ranges, devices, device groups.

7.2.3.4 FMT_MTD.1 (4) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 (4) The TSF shall restrict the ability to **[*perform the operations listed in column one of Table 7-8*]** the [***TSF data listed in column two of Table 7-8]*** to [***the assigned roles listed in column three of Table 7-8***].

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

Operations	TSF Data	Assigned Role
Create, Modify, Delete	All passwords	Administrator with Administrator Management extended privileges
Modify	Own password	System Administrator, End User
Create, Delete	Users	Administrator
Create, Delete	Administrators	Administrator
Assign, Modify	Allowed Devices by Range or Group	Administrator
Create, Modify, Delete	Groups of Devices	Administrator

Table 7-8: Operations Performed by Assigned Roles

Application Note: *User passwords must originally be created by the Administrator, with the User being able to change the password at a later time.*

7.2.3.5 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 management functions:

a) **[*All operations defined in Tables 7-6, 7-7, and 7-8*].**

Dependencies: No dependencies.

7.2.4 Trusted Path/Channel (FTP)

7.2.4.1 FTP_TRP.1 Trusted Path

Hierarchical to: No other components

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [**remote**] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [**modification, disclosure, [none]]**.

FTP_TRP.1.2 The TSF shall permit [**remote users**] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [**initial user authentication, [*management of the TOE and its data*]].**

Dependencies: No dependencies.

7.3 Operations Defined

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

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

- Assignment: allows the specification of an identified parameter. Indicated with ***bold text and italics*** if further operations are necessary by the Security Target author;
- Refinement: allows the addition of details. Indicated with ***bold text and italics*** if further operations are necessary by the Security Target author;
- Selection: allows the specification of one or more elements from a list. Indicated with <u>underlined text</u>; and
- Iteration: allows a component to be used more than once with varying operations. Not used in this PP.

In addition, this ST has extended requirements, as stated in the IDS System PP v1.7. These new requirements are indicated in bold text and contain the text (EXT) in the title.

8 Security Assurance Requirements

This section identifies the Security Assurance Requirement components met by the TOE. These assurance components meet the requirements for EAL3 augmented with ALC_FLR.2.

8.1 Security Architecture

8.1.1 Security Architecture Description (ADV_ARC.1)

ADV_ARC.1.1D: The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D: The developer shall design and implement the TSF so that it is able to protect itself from tampering by un-trusted active entities.

ADV_ARC.1.3D: The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1C: The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C: The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C: The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1.4C: The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C: The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

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

8.1.2 Functional Specification with Complete Summary (ADV_FSP.3)

ADV_FSP.3.1D The developer shall provide a functional specification.

ADV_FSP.3.2D The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.3.1C The functional specification shall completely represent the TSF.

ADV_FSP.3.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.3.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.3.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.3.5C For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from security enforcing effects and exceptions associated with invocation of the TSFI.

ADV_FSP.3.6C The functional specification shall summarize the SFR-supporting and SFR-non-interfering actions associated with each TSFI.

ADV_FSP.3.7C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

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

ADV_FSP.3.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

8.1.3 Architectural Design (ADV_TDS.2)

ADV_TDS.2.1D The developer shall provide the design of the TOE.

ADV_TDS.2.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

ADV_TDS.2.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.2.2C The design shall identify all subsystems of the TSF.

ADV_TDS.2.3C The design shall describe the behavior of each SFR non interfering subsystem of the TSF in detail sufficient to determine that it is SFR non-interfering.

ADV_TDS.2.4C The design shall describe the SFR-enforcing behavior of the SFR enforcing subsystems.

ADV_TDS.2.5C The design shall summarize the SFR-supporting and SFR-non interfering behavior of the SFR-enforcing subsystems.

ADV_TDS.2.6C The design shall summarize the behavior of the SFR-supporting subsystems.

ADV_TDS.2.7C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.2.8C The mapping shall demonstrate that all behavior described in the TOE design is mapped to the TSFIs that invoke it.

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

ADV_TDS.2.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

8.2 Guidance Documents

8.2.1 Operational user guidance (AGD_OPE.1)

AGD_OPE.1.1D The developer shall provide operational user guidance.

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

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

8.2.2 Preparative Procedures (AGD_PRE.1)

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

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

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

8.3 Lifecycle Support

8.3.1 Authorization Controls (ALC_CMC.3)

ALC_CMC.3.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.3.2D The developer shall provide the CM documentation.

ALC_CMC.3.3D The developer shall use a CM system.

ALC_CMC.3.1C The TOE shall be labeled with its unique reference.

ALC_CMC.3.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.3.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.3.4C The CM system shall provide measures such that only authorized changes are made to the configuration items.

ALC_CMC.3.5C The CM documentation shall include a CM plan.

ALC_CMC.3.6C The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.3.7C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.3.8C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

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

8.3.2 CM Scope (ALC_CMS.3)

ALC_CMS.3.1D The developer shall provide a configuration list for the TOE.

ALC_CMS.3.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; and the implementation representation.

ALC_CMS.3.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.3.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item. Evaluator action elements:

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

8.3.3 Delivery Procedures (ALC_DEL.1)

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

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

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

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

8.3.4 Identification of Security Measures (ALC_DVS.1)

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

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

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

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

8.3.5 Life-cycle Definition (ALC_LCD.1)

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

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

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

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

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

8.3.6 Flaw reporting procedures (ALC_FLR.2)

ALC_FLR.2.1D The developer shall document flaw remediation procedures addressed to TOE developers.

ALC_FLR.2.2D The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

ALC_FLR.2.3D The developer shall provide flaw remediation guidance addressed to TOE users.

ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.2.5C The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.2.6C The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.

ALC_FLR.2.7C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.2.8C The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

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

8.4 Security Target Evaluation

8.4.1 Conformance Claims (ASE_CCL.1)

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

8.4.2 Extended Components Definition (ASE_ECD.1)

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

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

ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

8.4.3 ST Introduction (ASE_INT.1)

ASE_INT.1.1D The developer shall provide an ST introduction.

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summarize the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

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

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

8.4.4 Security Objectives (ASE_OBJ.2)

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide security objectives rationale.

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

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

8.4.5 Security Requirements (ASE_REQ.2)

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirement’s rationale.

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

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

8.4.6 Security Problem Definition (ASE_SPD.1)

ASE_SPD.1.1D The developer shall provide a security problem definition.

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C The security problem definition shall describe the OSPs.

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

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

8.4.7 TOE Summary Specification (ASE_TSS.1)

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

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

ASE_TSS.1.2E The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

8.5 Tests

8.5.1 Analysis of Coverage (ATE_COV.2)

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

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

8.5.2 Basic Design (ATE_DPT.1)

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

ATE_DPT.1.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems in the TOE design.

ATE_DPT.1.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

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

8.5.3 Functional Tests (ATE_FUN.1)

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

ATE_FUN.1.2D The developer shall provide test documentation

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

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

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

8.5.4 Independent Testing (ATE_IND.2)

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

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

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

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

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

8.6 Vulnerability Assessment

8.6.1 Vulnerability Analysis (AVA_VAN.2)

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

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

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

AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

9 TOE Summary Specification

9.1 TOE Security Functions

The following sections identify the security functions of the TOE. They include Security Audit, Identification and Authentication, Security Management, Protection of the TSF, Intrusion Detection System, and Encrypted Communications.

9.1.1 Security Audit

The TOE creates audit events, or syslogs for all actions taken within QRadar. These events are stored in the TOE's internal database and can be viewed by users with the System Administrator privilege. The syslog audit records are sent via loopback between components within the TOE's QRadar Console. Although this information never leaves the machine on which the QRadar Console is installed, there is a reliance on the operational environment's OS and machine to assist the TOE in protecting the confidentiality and integrity of the transmitted syslog audit messages.

Additionally, the TOE also writes audit records to Apache event log files located on the local Operating System. These audit records also require the operational environment's OS to protect this data. The local audit data cannot be accessed via the TOE once it is written to the Apache event log files and requires local access to the OS to read these files.

The following sections describe the audit events in more detail.

9.1.1.1 Audited Events and Storage

The TOE logs all QRadar actions, with the following parameters: Date and time, Host name, User and IP address, Thread ID, Category, Sub-category, Action, and Payload. The TOE provides reliable timestamps to be used in the TOE's audit events. The complete list of audited events can be found in the table below. The audit events created from these events are stored to the TOE's internal database.

Category	Action	Test Case ID
User Authentication	Log in to QRadar	qr-3721, qr-3722, qr-3742
	Log out of QRadar	
Administrator Authentication	Log in to the QRadar Administration Console	qr-3722, qr-3724
	Log out of the QRadar Administration Console	
System Management	Shutdown a system	qr-3927
	Restart a system	qr-3926
Session Authentication	Create a new administration session	
	Terminate an administration session	
	Deny an invalid authentication session	
	Expire a session authentication	
	Create an authentication session	
	Terminate an authentication session	

Rules	Add a rule	qr-3968
	Delete a rule	qr-3971
	Edit a rule	qr-3970
User Accounts	Add an account	qr-2750
	Edit an account	qr-3797
	Delete an account	qr-3796
User Roles	Add a role	qr-2750
	Edit a role	qr-3791
	Delete a role	qr-3796
Log Sources	Add a log source	qr-3785
	Edit a log source	qr3789
	Delete a log source	qr-3788
	Disable a log source	qr-3848
	Enable a log source	
	Add a log source to a group	qr-2845
	Delete a log source from a group	qr-2844
	Edit the DSM parsing order	qr-3873
Log Source Extension	Add a log source extension	qr-3957
	Edit the log source extension	qr-3964
	Delete a log source extension	qr-3965
	Copy a log source extension	qr-3960
	Upload a log source extension successfully	qr-3957
	Upload an invalid log source extension	qr-3961
	Download a log source extension	qr-3958
	Report a log source extension	qr-3962
	Modify a log source's association to a device or device type	qr-3967
Flow Sources	Add a flow source	qr-3972
	Edit a flow source	qr-3974
	Delete a flow source	qr-3975
	Disable a flow source	qr-3973
	Enable a flow source	
Offenses	Hide an offense	qr-3922
	Close an offense	qr-3923
	Close all offenses	qr-3924
Syslog Forwarding	Add a syslog forwarding	qr-3978
	Delete a syslog forwarding	qr-3980
	Edit a syslog forwarding	qr-3979
Reports	Add a template	qr-3928
	Delete a template	qr-3955
	Edit a template	qr-3950
	Execute a template	qr-3929
	Delete a report	qr-3956
	Download (view) a report	qr-2954
Groups	Add a log source group	qr-2841
	Delete a log source group	qr-2842
	Edit a log source group	qr-3790
VIS	Discover a new host	qr-3977
	Discover a new operating system	
	Discover a new port	
	Discover a new vulnerability	
Scanner	Add a scanner	qr-3916

	Delete a scanner	qr-3921
	Edit a scanner	qr-3917
Scanner Schedule	Add a schedule	qr-3918
	Edit a schedule	qr-3919
	Delete a schedule	qr-3920
SIM	Clean a SIM model	qr-3976
Asset	Delete all assets	qr-3887
Database Properties	Add a custom event property	qr-3888
	Edit a custom event property	qr-3907
	Delete a custom property	qr-3908
Database Property Extensions	Add a custom event property expression	qr-3888
	Edit a custom event property expression	qr-3907
	Delete a custom event property expression	qr-3908
Installation	Install a .rpm package, such as a DSM update	qr-2813

Table 9-1: Logged Actions

All of the audited events listed in Table 9-1 are actions that users take upon the TOE. These events are recorded as audit data and are stored in a location separate from where IDS event logs are stored.

Audit logs are in a plain text format and are compressed in an archive once the audit log file size exceeds 200 MB. The default/current audit log file name is "audit.log." The archive naming scheme names audit log files as "audit.log.#.gz," where # is a number that starts at 1 and is incremented for each audit log file that is archived. Compressed files are kept for 50 weeks before being deleted. When an audit is compressed a new "audit.log" file is created, which is also archived once it exceeds 200 MB in size. When a log is compressed, audit.log.n.gz becomes audit.log.n+1.gz. For instance, audit.log.1.gz becomes audit.log.2.gz. Audit.log becomes audit.log.1.gz and a new audit.log file is created. The audit log storage is located on a separate partition from the IDS storage. This partition is passively monitored by default but can be configured to be actively monitored. Passive monitoring means that if the partition is full QRadar will continue to function. Audit logs will not be generated but audit events will continue to be generated. There is a total of 2 TB available for storage. When the audit log trail becomes full, manual intervention is required and the TOE sends first a warning and then an alarm to the configured user via email. If actively monitored, rather than passively, QRadar processes are shutdown to prevent corruption when the maximum threshold is reached or exceeded.

9.1.1.2 Audit Review

Only users with the System Administrator privilege are able to view audit events from the QRadar Console User Interface. All other users are denied access to the audit events. No users on the TOE are authorized to delete audit events. Since the user and IP address that edits any aspect of QRadar or its audit events is recorded for each modification, modifications are also easily detected. Once the audit storage becomes full, the TOE ensures that the most recent events are maintained. Audit event retention is determined by the retention period set for the internal event database, which is defaulted to 30 days, but is configurable by the administrator. Only users with root access to the TOE appliance can locally access the logs; however, this is not supported in the evaluated configuration.

The set of audited events cannot be selected; everything that is audited is audited all the time. Auditable event data is generated and stored on the QRadar Console, where it can be viewed in a report format. The QRadar Console can be accessed through Internet Explorer 7.0 or higher or Mozilla Firefox 3.6 or higher browsers. When viewing audit events, the System Administrator is able to sort the data based on the following parameters: ascending or descending for date and time, subject identity (in this case user and IP address), type of event (in this case category and sub-category), and success or failure verdict. Additionally, the audit events can be displayed based on an inputted event type, as well as the following normalized event fields:

Source or Destination IP	Category	Destination Asset Name
Destination IP	Destination Port	Log Source
Log Source Group	Source Asset Name	Source IP
Event Name	Associated With Offense	Credibility
Custom Rule	Custom Rule Partial Matched	Destination MAC
Destination Network	Destination Network Group	Duplicate
Direction	Duration	End Time
End Date	Event Count	Event Processor
Event Is Unparsed	Geographic Country	Geographic Region
High Level Category	IPv6 Destination	IPv6 Source
Is CRE Event	Identity Username	Identity IP
Identity MAC	Identity Hostname	Identity Net Bios Name
Identity Group Name	Identity Extended Field	Has Identity
Log Source Time	Log Source Date	Log Source Type
Magnitude	Payload	Post NAT Destination IP
Post NAT Destination Port	Post NAT Source IP	Post NAT Source Port
Pre NAT Destination IP	Pre NAT Destination Port	Pre NAT Source IP
Pre NAT Source Port	Protocol	Relevance
Remote Network	Remote Network Group	Remote Service
Remote Service Group	Severity	Source MAC
Source Network	Source Network Group	Source Port
Source or Destination Network	Source or Destination Port	Start Time
Start Date	Username	Any user-defined field

Table 9-2: Normalized Event Fields

Audit logs are displayed in the following format: <date_time> <host ip> <user>@<IP address> (thread ID) [<category>] [<sub-category>] [<action>] <payload>. The maximum audit log size is 1024 characters.

9.1.2 Identification and Authentication

The TOE uses OpenSSH to authenticate to and secure its communication with Q1 Labs for patch and/or IDS definition updates used by the TOE. The Q1 Labs server to QRadar connection involves the authorization of a manifest file that resides on the Q1 Labs server. The QRadar appliance verifies the integrity of this manifest file, and will disallow any update information from a server that fails this check. All patch update information must be manually applied by an Administrator within the evaluated configuration..

The TOE requires that all users of the TOE be identified and authenticated before access is granted to the TOE and its resources. Authentication must first be configured by an administrator, and no actions are allowed on the TOE prior to a user being identified and authenticated. When five unsuccessful authentication attempts have been reached within a 10 minute timeframe, the host from where the attempt was made is locked out for 30 minutes. The number of unsuccessful attempts (default 5), the time period in which the attempts occur (default 10 minutes) and the amount of time the user is locked out (default 30 minutes) are all configurable by the Administrator.

All users enter a valid username and password combination via a web browser in order to access the TOE via the QRadar Console. The TOE ensures that certain security attributes are maintained for all users – which aid in the process of proper identification and privilege assignment. Security attributes maintained for end users include the following: username, authentication data, CIDR address ranges, devices, device groups, and assigned privileges. The TOE also maintains the following security attributes for administrators: username, authentication data, and assigned role. TOE users are not related to users of the underlying operating system of the TOE installation. In addition, TOE users are not related to users of any other IT system or enterprise structure within the evaluated configuration.

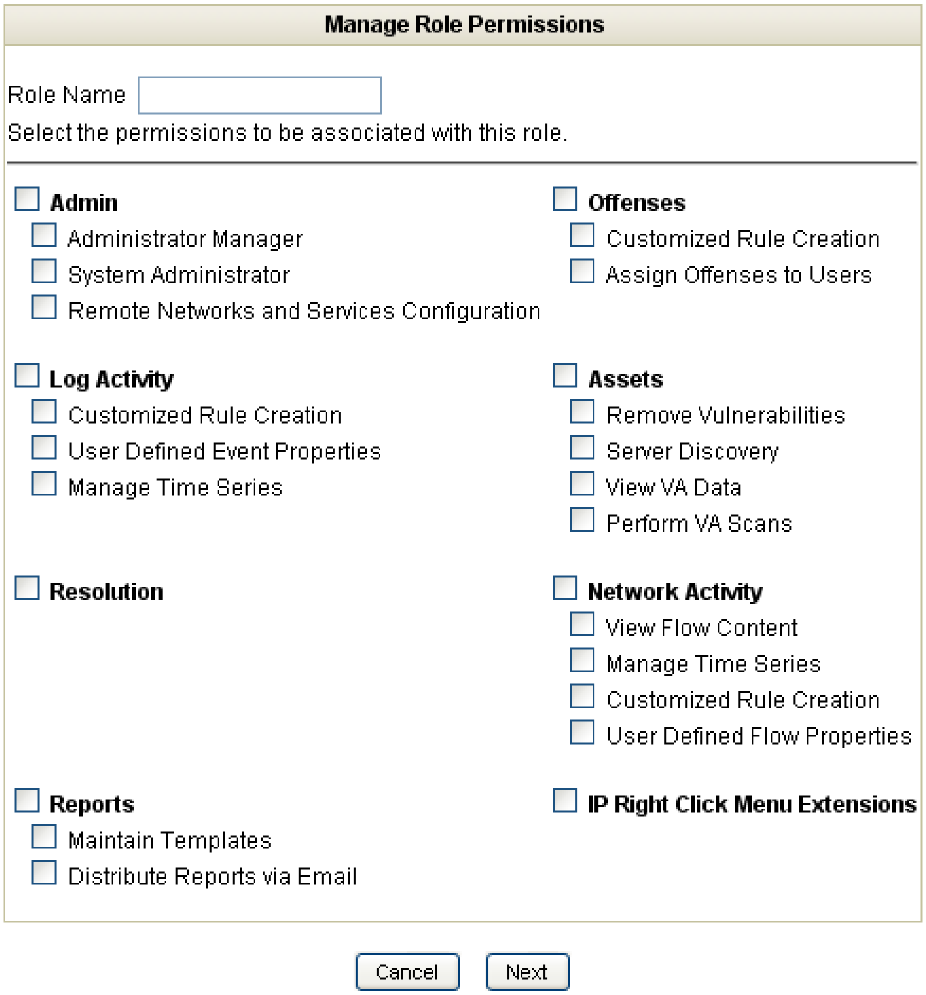
Once the TOE verifies a user's authentication data, the user is authorized to perform functions on the TOE based on his or her assigned privileges. These privileges are granted by an administrator with the Administrator Manager extended privilege. Refer to tables 7-6, 7-7, and 7-8 for TOE operations that require special privileges.

When the TOE is freshly installed, it contains a default account of the role Administrator. This default account can be modified from its original configuration, making it exactly the same as any other user account on the TOE. This default Administrator account contains the privileges to configure additional roles and users, and therefore has the capability to set up TOE users as per the requirements set by this document.

9.1.3 Security Management

The TOE maintains three roles – Administrators, System Administrators, and End Users. An administrator role must first be created by the primary Administrator before any user account can be created. Once user accounts are created, each account must be associated with a role. Permissions, or privileges, are assigned to the following roles maintained by the TOE: Administrators, System Administrators, and End Users. These privileges determine what a user can do on the TOE based on his or her role. An end user is someone who belongs to a non-administrative role. The privileges assigned to this role are defined by the Administrator. An End User with no privileges can perform the following functions on the TOE: query a pre-defined Dashboard (see Section 9.1.3.3), query IDS event data, and modify his or her own password. An Administrator role has all of the Admin extended privileges enabled for his or her account. System Administrators can only configure System data collection standards/protocols and basic

QRadar functionality. However, System Administrators cannot edit Administrator user accounts, and can change their own password. See Table 9-3 and 9-4 for more information on roles and privileges.



Manage Role Permissions

Role Name

Select the permissions to be associated with this role.

- □ **Admin**
  - □ Administrator Manager
  - □ System Administrator
  - □ Remote Networks and Services Configuration
- □ **Offenses**
  - □ Customized Rule Creation
  - □ Assign Offenses to Users
- □ **Log Activity**
  - □ Customized Rule Creation
  - □ User Defined Event Properties
  - □ Manage Time Series
- □ **Assets**
  - □ Remove Vulnerabilities
  - □ Server Discovery
  - □ View VA Data
  - □ Perform VA Scans
- □ **Resolution**
- □ **Network Activity**
  - □ View Flow Content
  - □ Manage Time Series
  - □ Customized Rule Creation
  - □ User Defined Flow Properties
- □ **Reports**
  - □ Maintain Templates
  - □ Distribute Reports via Email
- □ **IP Right Click Menu Extensions**

Figure 2 – QRadar Role Permissions Dialog

Roles are custom named templates that include any number of system privileges, shown in Figure 2. For example, a user can be assigned a "Log Activity Supervisor" role, where the Log Activity privilege is checked. Therefore, any number of user roles can be granted access to audit events.

Table 9-3 below details the extended privileges that are linked to each of the privileges:

Privilege	Extended Privilege Description
Admin	Within the administrator role, users can be granted additional access to the following: • Administrator Manager - Allows users the ability to create and edit other administrative user accounts. If this check box is selected, the System Administrator check box is automatically selected. • System Administrator - Allows users access to all areas of QRadar except Remote Networks and Remote Services Configuration.. Users with this access are not able to edit other Administrator user accounts. • Remote Networks and Services Configuration - Allows users the ability to create, edit, or delete Remote Networks and/or Remote Services..
Offenses	Within the Offenses interface functionality, users can be granted additional access to the following: • Customized Rule Creation - Allows users to create custom rules. • Assign Offenses to Users - Allows users to assign offenses to other users.
Log Activity	Within the Log Activity role, users can be granted additional access to the following: • Customized Rule Creation - Allows users to create rules using the Events interface. • User Defined Event Properties - Allows users the ability to create user-defined event properties. • Manage Time Series
Assets	Within the Asset Management functionality, users can be granted additional access to the following: • Remote Vulnerabilities • Server Discovery - Allows users the ability to discover servers. • View VA Data - Allows users access to vulnerability assessment data. • Perform VA Scans - Allows users to perform vulnerability assessment scans.

Network Activity	Grants users' access to Network Activity functionality. Within the Network Activity functionality, additional access can be granted to the following: • View Flow Content - Grants users' access to data accessed through the View Flow function. • Manage Time Series • Customized Rule Creation - Allows users to create rules using the Network Activity interface. • User Defined Flow Properties
Reports	Select the check box to grant this user access to Reporting functionality. Within the Reporting functionality, users can be granted additional access to the following: • Maintain Templates - Allows users to maintain reporting templates. • Distribute Reports via Email - Allows users to distribute reports through e-mail.
IP Right Click Menu Extensions	No extended privileges.

Table 9-3: Privileges with Associated Extended Privileges

The following table shows the privileges associated with each role.

User	Privileges
Authorized System Administrator	• Configure System data collection standards/protocols • Configure basic QRadar functionality • Change own password • Edit non-administrator user accounts *Note: System Administrator extended privilege gives all end user privileges.*
Authorized Administrator	Admin privilege, any subset of the admin extended privileges: Administrator Manager, System Administrator, Views Administrator
End User	Any subset of the following privileges: Offenses, Log Activity, Assets, Resolution, Network Activity, and Reports privileges and all related extended privileges

Table 9-4: Defined User types and required/allowed privileges

Other privileges that are available for assignment to users are Offenses, Offenses with Customized Rule Creation, Reports, Log Activity, Log Activity with Customized Rule Creation, Network Activity, Network Activity with Customized Rule Creation, and other custom privileges defined by an administrator.

Administrators also have the ability to occupy more granular roles such as: Administrator Manager, Remote Networks and Services Configuration, and System Administrator. In essence, there can be any number of Administrators with varying capabilities (i.e. according to the privileges that have been assigned to them). Administrators who have the necessary privileges assigned have the ability to perform management functions. Among the management functions that can be performed are:

- Manage users
- Manage network settings
- Manage QRadar settings
- Manage authorized services
- Manage deployment views
- Manage flow sources
- Configure sentries
- Configure views
- Configure syslog forwarding
- Managing vulnerability scanners
- Configure the Resolution module
- Manage log sources
- Perform IDS definition updates by utilizing Q1 update servers

Note: QRadar also allows authorized users the ability to perform patch updates by utilizing the Q1 update servers. These patch updates are completely separate from signature updates. In the evaluated configuration, all patch update information must be manually applied by an Administrator.

Listed below are the abilities specific users can perform along with the necessary privileges:

Operations Selection and Assignment	TSF Data Assignment	Privilege Assignment
Query	Pre-defined Dashboard Report	Users
View	Audit Events	Users with System Administrator privileges

Query, Modify, Delete, Create	Reporting interface to System data	Users with Reports privileges
Query, Modify, Delete, Create	Configuration for rules applied to the System data from which Alerts (IDS_RCT.1) are generated, includes email notification and logging.	Users with Log Activity, Offenses or Network Activity with Customized Rule Creation privileges
Query	System data (Flow data)	
Query	Events	Users with Log Activity privileges

Table 9-5: User Privilege Assignments

Users with no privileges assigned only have the ability to change their password. Administrators granted the Administrator Management privilege can create, modify, and delete any and all passwords.

Administrators are also able to manage System data contained in the specified CIDR ranges for each user. CIDR, or Classless Inter-Domain Routing, is an addressing scheme for the internet that allocates internet addresses used in inter-domain routing. By using CIDR, a single IP address can be used to designate many unique IP addresses. CIDR address ranges, devices, and device groups are used to determine which devices a user can perform management functions against.

9.1.3.1 Rules

Rules match events or offenses by performing a series of tests. If all the conditions of a test are true, the rule generates a response. Using the Log Activity, Offenses or Network Activity interfaces, administrators can configure rules or building blocks. Building blocks are rules without a response. Possible responses to a rule include:

- Create an offense
- Generate a response to an external system (syslog or SNMP trap)
- Send an e-mail
- Generate system notifications using the Dashboard

The tests in each rule can also reference other building blocks and rules. Rules do not need to be created in any specific order since the system checks for dependencies each time a new rule is added, edited, or deleted. If a rule that is referenced by another rule is deleted or disabled, a warning appears and action is not taken. Each rule may contain the following components:

- Functions - With functions, administrators can use building blocks and other rules to create a multi-event or multi-offense function. Administrators can also OR rules together, using them when the Administrator sees an event match any of the following rules function.
- Building blocks - A building block is a rule without a response and is used as a common variable in multiple rules or to build complex rules or logic that

administrators want to use in other rules. A group of tests can be saved as building blocks for use with other functions. Building blocks allow administrators to re-use specific rule tests in other rules. For example, a building block that includes the IP addresses of all mail servers in the network can be saved and then use that building block to exclude those hosts from another rule. The building block defaults are provided as guidelines, which should be reviewed and edited based on the needs of the network.

- Tests - Property of an event or an offense, such as a source IP address, severity of event, or rate analysis. A user with non-administrative access can create rules for areas of the network that they have access. Users must have the appropriate permission access to manage rules.

The following rule types can be configured:

- Event Rule - An event rule performs tests on events as they are processed in real-time by the Event Processor. Administrators can create an event rule to detect a single event (within certain properties) or event sequences. For example, if an administrator wants to monitor the network for invalid login attempts, access multiple hosts, or a reconnaissance event followed by an exploit, the administrator can create an event rule. It is common for event rules to create offenses as a response.
- Flow Rule - A flow rule performs tests on flows as they are processed in real-time by the QFlow Collector. Administrators can create a flow rule to detect a single flow (within certain properties) or flow sequences. It is common for flow rules to create offenses as a response.
- Events and Flow Rule - A common rule performs tests on fields that are common to both event and flow records. For example, an administrator can create a common rule to detect events and flows that have a specific source IP. It is common for common rules to create offenses as a response.
- Offense Rule - An offense rule processes offenses only when changes are made to the offense, such as, when new events are added or the system scheduled the offense for reassessment.

9.1.3.2 QRadar Console User Interface

The QRadar Console User Interface serves as the primary interface where both administrators and users can modify, query, delete, and create information (so long as they have the requisite privileges assigned to them). In addition, this interface allows System Administrators to configure the System data collection, analysis, and reaction. The QRadar Console User Interface provides real-time views, reports, alerts, and in-depth investigation of flows for network traffic and security threats. The QRadar Console is accessed through a web browser, i.e. Internet Explorer 7.0 or higher and Mozilla Firefox 3.6 or higher.

The QRadar Console utilizes pre-analyzed data derived by its internal engine to populate the user interface. The QRadar Console User Interface screen includes the Dashboard view, the Offences view, the Log Activity view, the Assets view, the Network Activity view, the Reports view, and the Admin view.

- 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.
- The Offences interface provides a prioritized list of offenses based on all log, flow, and vulnerability data analyzed. From the Offenses interface, administrators can investigate an offense to determine the root cause of an issue. This tab also displays the alerts when they are written to the QRadar Console.
- The Log Activity interface allows users to view event logs being sent to QRadar in real-time or through searches. This interface is used for performing in-depth investigations on IDS event data and for identifying false positive and tuning QRadar.
- The Assets interface is used by QRadar to automatically discover assets (servers and hosts) operating on the network. This is based on passive System data (specifically flow data and vulnerability data), which allows QRadar to build an asset profile. Asset profiles display the services running on each asset. This profile data is used for correlation purposes to help reduce false positives.
- The Network Activity interface allows users to monitor and investigate System data (specifically flow data) in real-time, or perform advanced searches. A flow is a communication session between two hosts. Viewing flow information allows a user to determine how the traffic is communicated, what is communicated, and includes such details as when, who, how much, protocols, ASN values, IfIndex values, or priorities.
- The Reports interface allows users to create, distribute, and manage reports for any data within QRadar. This view allows users to create customized reports where information can be combined into a single report. The pre-installed report templates that are included with QRadar can also be used.
- The Admin interface can only be accessed by administrators. The Admin interface is used by administrators to do the following:
    - System Configuration - Allows administrators to configure system wide QRadar settings including, users, thresholds, system settings, network hierarchy, authentication, sentries, backup and recovery, Console settings, or automatic IDS definition updates.
    - Data Sources - Allows administrators to configure log sources, syslog forwarding, flow sources, and scanners.

- Remote Networks and Services Configuration - Allows administrators to create remote networks and remote services for use in the custom rules engine and in flow and event searches. Remote network and service groups enable the administrator to represent traffic activity on the network for a specific profile.

- Deployment editor - Allows administrators to manage the individual subsystems of the QRadar deployment. The Deployment Editor is used to create the deployment, assign connections, and configure each subsystem. The Deployment Editor provides the following views of a deployment:

  - System View – Allows administrators to assign software components, such as a QFlow Collector, to systems (managed hosts) in a deployment. The System View includes all managed hosts in a deployment.

  - Event View – Allows administrators to create a view for the SIM components including QFlow Collectors, Event Processors, Event Collectors, and Magistrate components.

The Dashboard is the default view when logging into QRadar. The Dashboard provides a workspace environment that supports multiple dashboards on which users can display views of network security, activity, or data that QRadar collects according to the user's responsibility. The Dashboard interface provides default dashboards focused on security, network activity, application activity, and compliance. Users can create custom dashboards that are relevant to their responsibilities.

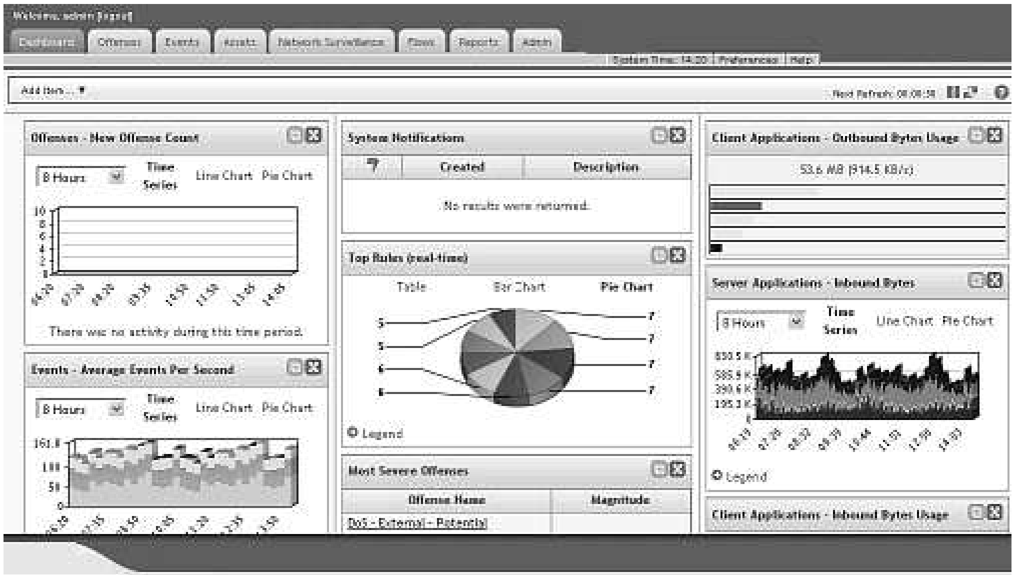


Figure 3 – Dashboard View

As illustrated in Figure 3, the Dashboard provides users with a graphical representation of offense metrics as well as log and network activity information. The table below details each Dashboard item as well as the Privileges necessary to view those items:

Dashboard Item			Required Privilege
Offenses	Offenses	• Most Severe Offenses • Most Recent Offenses • My Offenses • New Offenses Over Time	Offenses
	Attackers and Targets	• Top Attackers • Top Local Targets	Offenses
	Categories	Top Category Types	
Events		Event Searches	Events * List of searches if available for viewing on the Dashboard
		Events Over Time	Events
		Events by Severity	
		Top Log Sources	
Resolution		Recently Deployed Actions	Resolution
Reports	Most Recent Reports		Reports
Enterprise Security State			Administrator
Enterprise Vulnerability State			
System Summary			Administrator and System Administrator
System Notifications			Configured user

Table 9-6: Dashboard Options and Necessary Privileges

9.1.3.3 Managing Users

Administrators have the ability to manage users and their accounts. Multiple accounts with administrative privileges can be created for a system. Only the primary administrative account can create accounts that have administrative privileges. Any type of user account can be added or removed for any individual that requires access to the TOE. Each user must first be associated with a role, which aids in determining the privileges that user can operate under. Administrators also have the ability to restrict or allow access to specific areas of the network.

As shown in Table 7-8, users with the administrative privilege (including the default administrative role), can view existing user roles, create a role, edit a role, and delete a role through the QRadar Console User Interface.

Administrators can specify which network objects they want to assign users. This affects the events that appear in the Log Activity interface of Dashboard. The options include:

- Network only – A user must have access to either the source network or the destination network of the event to have the event appear in the Log Activity interface.

- Devices only – A user must have access to either the device or device group that created the event to have the event appear in the Log Activity interface.

- Networks and Devices – A user must have access to both the source or the destination network and the device or device group to have an event appear in the Log Activity interface.

- All – All events appear in the Events interface. Any user with Log Activity role permissions is able to view all events allowed by the role, a non-administrator role is configured so that audit events cannot be viewed by non-admin users.

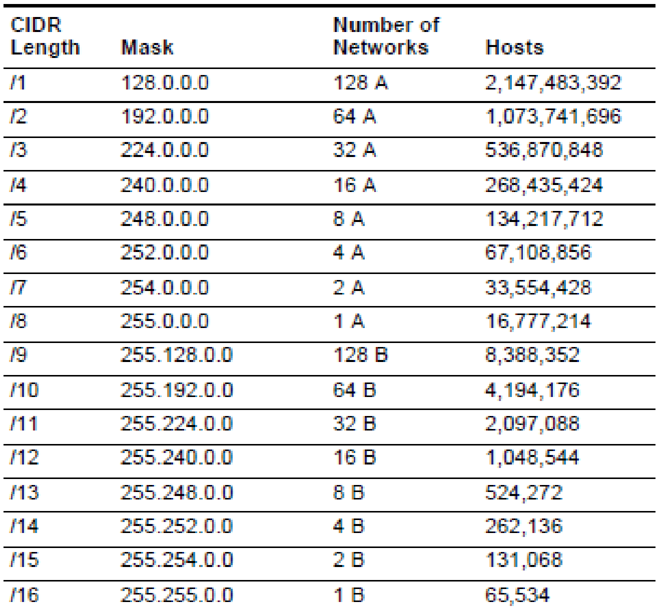
9.1.3.4 System Management

The TOE uses a network hierarchy to understand network traffic and provide the ability to view network activity for an entire deployment. When developing a network hierarchy, the most effective method for viewing network activity should be considered. It is important to note that when configuring the TOE, QRadar currently only supports IPv4 networks. QRadar cannot build out network objects based on IPv6 addressing. However, QRadar can still monitor, report, and correlate IPv6 data. A network can be based on many different variables, including geographical or business units.

Multiple Classless Inter-Domain Routings (CIDRs) or subnets can be combined into a single network/group to conserve disk space.

The TOE maintains a list of acceptable CIDR values for network objects. This list is shown below:

Table 4-2 Accepted CIDR Values



CIDR Length	Mask	Number of Networks	Hosts
/1	128.0.0.0	128 A	2,147,483,392
/2	192.0.0.0	64 A	1,073,741,696
/3	224.0.0.0	32 A	536,870,848
/4	240.0.0.0	16 A	268,435,424
/5	248.0.0.0	8 A	134,217,712
/6	252.0.0.0	4 A	67,108,856
/7	254.0.0.0	2 A	33,554,428
/8	255.0.0.0	1 A	16,777,214
/9	255.128.0.0	128 B	8,388,352
/10	255.192.0.0	64 B	4,194,176
/11	255.224.0.0	32 B	2,097,088
/12	255.240.0.0	16 B	1,048,544
/13	255.248.0.0	8 B	524,272
/14	255.252.0.0	4 B	262,136
/15	255.254.0.0	2 B	131,068
/16	255.255.0.0	1 B	65,534

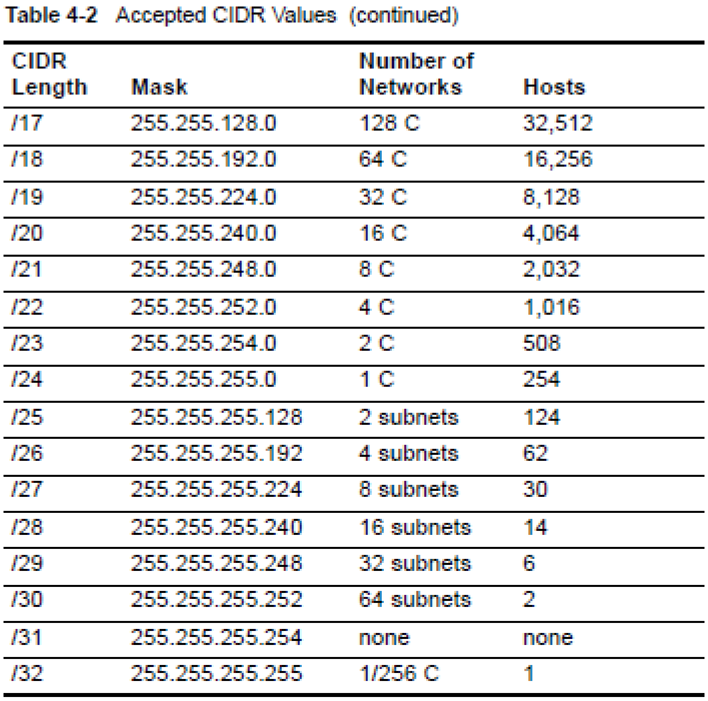


Table 4-2 Accepted CIDR Values (continued)

CIDR Length	Mask	Number of Networks	Hosts
/17	255.255.128.0	128 C	32,512
/18	255.255.192.0	64 C	16,256
/19	255.255.224.0	32 C	8,128
/20	255.255.240.0	16 C	4,064
/21	255.255.248.0	8 C	2,032
/22	255.255.252.0	4 C	1,016
/23	255.255.254.0	2 C	508
/24	255.255.255.0	1 C	254
/25	255.255.255.128	2 subnets	124
/26	255.255.255.192	4 subnets	62
/27	255.255.255.224	8 subnets	30
/28	255.255.255.240	16 subnets	14
/29	255.255.255.248	32 subnets	6
/30	255.255.255.252	64 subnets	2
/31	255.255.255.254	none	none
/32	255.255.255.255	1/256 C	1

Figure 4 – Accepted CIDR Values

9.1.4 Encrypted Communications

Remote users establish a session with the TOE using a web-based GUI that is secured via OpenSSL 0.9.8e. The SSL protocols used in the evaluated configuration are SSLv3 and TLSv1. This secured path is used for initial user authentication, as well as, TOE management and operations by Administrators, System Administrators, and End Users. This path ensures that all transferred TOE data is protected from modification and disclosure. The TOE uses 256-bit keys for encryption and decryption using the algorithm of AES in CBC mode in support of OpenSSL 0.9.8e for communication with remote users and for OpenSSH 4.3p2 between TOE subsystems. The SSH protocol used is protocol 2. This configuration is captured in RFC 3602. Additionally, the TOE generates 1024-bit RSA keys for key management in support of OpenSSH and OpenSSL as supported by RFC 4432. All keys are destroyed by the overwrite method when new keys are generated, and this is taken care of by the browser and/or Operating System.

9.1.5 Protection of the TSF

OpenSSH 0.9.8b is used by the TOE to protect the integrity and confidentiality of all TSF data during transmission between TOE subsystems. System data are made available from one TOE subsystem to another (i.e. a trusted remote IT product) immediately upon completion of a scanning session, given the following: reporting data files are in use during an active scanning session, scanner reporting data is in a flat file format, and availability to another TOE subsystem is predicated upon the correct file locking functionality.

The only method for users or administrators to access other subsystems associated with the TOE is through the QRadar Console; this access method cannot be circumvented. The TOE has the ability to detect any modifications that unauthorized users have made or attempt to make to data in transmission via secure hashing that uses HMAC-MD5. If the hash sent from one TOE subsystem does not match the hash computed by the receiving TOE subsystem, the TOE will drop the packet and request the packet to be retransmitted. When this occurs, a custom rule will detect the communication failure or an Administrator documents the data for the purpose of auditing or compliance.

9.1.6 Intrusion Detection System

The TOE is an Intrusion Detection System which is designed to detect any unwanted attempts at accessing, manipulating, and disabling associated networks. More specifically, QRadar collects a multitude of information for targeted IT System resources, such as:

- Start-up and Shutdown
- Identification and authentication events
- Data accesses
- Service requests
- Network Traffic
- Security Configuration Changes
- Data Introduction
- Detected malicious code
- Access control configuration
- Service Configuration
- Authentication Configuration
- Accountability policy configuration
- Detected known vulnerabilities
- System data (See Table 7-3 for further details)

At a minimum, the TOE records the following information for each event: date and time of the event, event type, subject identity, and the success or failure of the event. The information that is collected from targeted IT System Resources is distributed to groups – which are defined by an Administrator. For more information on the information that is collected, please refer to Table 7-4.

9.1.6.1 Data Collection and Processing

The Event Processor is responsible for the collection and consolidation of System data passed from the QFlow Collector. This subsystem has the ability to log valid communications from the attacking or infected host(s). This data is stored in the flow logs. The Event Processor is responsible for the removal of all duplicate flows and creates an aggregation of flows.

The Event Processor processes events collected from the Event Collector. Once received, the Event Processor correlates the information. The TOE performs tests on the events to determine factors such as vulnerability data, relevance of the targets, importance, or credibility of the events. The results of the tests appear as annotations in the Offenses and Events interfaces. Also, custom rules are applied to additional events for specific incident recognition. Once complete, the Event Processor stores the event in its database and, in some circumstances, performs real-time flow analysis to determine the appropriate routing of the event. For example, once the Event Processor receives an event, the TOE determines how to apply tests to the event. Once the tests are completed, the event is passed through the TOE's internal engine to determine the custom rules that apply to the event. The event is then passed through the TOE's internal database for storage and other internal modules to determine if real-time flow analysis should be performed and if the event should automatically generate a new offense or become part of an existing offense. If this is the case, the event is sent to the Magistrate inside the QRadar Console.

9.1.6.2 Analysis

In addition to collecting System data, the TOE is capable of analyzing this data. This is performed by the following TOE subsystems which contain analyzer modules: Managed Host – Events and Managed Host – Flows. The data collected is analyzed to determine if there are any correlations with overall behavior and events. Behavioral and event correlations map directly statistical, signature, and/or integrity data. Statistical analysis involves identifying deviations from normal patterns of behavior. For example, it may involve mean frequencies and measures of variability to identify abnormal usage. Signature analysis involves the use of patterns corresponding to known attacks or misuses of a System. For example, patterns of System settings and user activity can be compared against a database of known attacks. Integrity analysis involves comparing System settings or user activity at some point in time with those of another point in time to detect differences. Within each of the analyzed results, the TOE records the date and time of the result, the type of result rendered the identification information of the data source, and the overarching analysis results. This System data is collected by the QFlow Collector where it is then processed by the Event Processor. This analysis begins with the normalization of the flow, the removal of duplications, and finally by bundling the flows – further optimizing the analysis. This data is then tagged based on packet header data, threat configuration information, and policy configuration information.

Signatures (event and vulnerability mappings) within the TOE can be updated by an Administrator or System Administrator by utilizing the TOE signature update functionality. This functionality allows a connection to the Q1 servers to download updated signature information from the official servers. This updated signature information is then applied to the signatures utilized within the system.

If an intrusion or any other security, policy, or compliance violation has been detected after the analyzer has compiled and analyzed the System data, the System does one or more of the following: sends an alarm to either the QRadar Console User Interface (individuals must have the Offense privilege), to the QRadar system log, send a notification via email, or to a remote machine via SNMP trap.   QRadar will continue to monitor the Offense and update any information that changes relative to the incident (e.g. the attacker begins attacking other targets). Users can be notified by email if the Offense changes, if they so choose. In addition, an e-mail notification is sent every 1% increase beginning at 90% disk utilization for the internal database.

All users have the ability to read the TOE's collected System data.   The specific data a user is able to read is defined by his or her role and allowed devices by type, group or CIDR range. The users without the necessary authorizations (i.e. role) are not allowed access to read the System data. QRadar provides the following methods to view collected network traffic.

- Managing Remote Networks - Remote network groups display user traffic originating from named remote networks. Users who have been assigned the administrator role can create remote network groups, aggregate flow and event search results on remote network groups and create rules that test for activity on remote network groups.

- Managing Remote Services - Remote services groups organize traffic originating from user-defined network ranges or, if desired, the Q1 Labs automatic update server. Once remote service groups are created, users who have been assigned the administrator role can aggregate flow and event search results and create rules that test for activity on remote service groups.

- The other method is known as the Reports privilege. 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 chart type determines how the generated report presents data and network objects. The following chart types are available for each report:

    - Asset Vulnerabilities
    - Connections
    - Event/Logs
    - Flows
    - Top Destination IPs
    - Top Offenses
    - Top Source IPs

9.1.6.3 Protecting System Data

The TOE is responsible for ensuring that System data is protected from unauthorized deletion or modification by users not possessing the requisite privileges. It is important to note, however, that authorized deletion of data is not considered a modification of System data in this context.

QRadar stores the System data in 2 separate databases:

- Postgres SQL database on each subsystem. This database is used to store configuration information. Postrgres is open source, and is in /store/postgres.
- Internal TOE database. This database is used to store raw System data for auditing and reporting.

The System data is stored in an internal file-based database on the TOE's internal engine server to a location specified by a System Administrator. The default location is /store/ariel/flows and is configurable. The post-analysis and raw event data is stored on the TOE's internal engine server in an internal proprietary TOE database. QRadar protects the stored System data from unauthorized modification and deletion through the TSF interfaces. The TOE is engineered so that the user cannot delete or modify the System data. All users are authorized to read the System data from the System data store.

The TOE ensures that when the storage capacity is nearing exhaustion that the most recent System data is maintained. The following thresholds are defined:

- Start compressing events and flows at 15% free disk space, stop compressing at 18%
- Start deleting events and flows at 17% free disk space, and stop deleting at 19%. This goes from oldest data to newest.

When the disk space utilization of the database server exceeds the warning and maximum thresholds an email notification is sent for both events. A notice is also sent at each 1% increment in disk space until the disk space utilization has 19% free space. If 95% or higher disk utilization occurs on an actively monitored partition QRadar will shutdown to avoid file corruption. QRadar will resume normal operation if by compression and deletion of files 19% or more disk space if freed. 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 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 administrator is responsible to configure and adjust the expiry data so that older data does not saturate the internal engine server's storage capacity.

9.2 TOE Summary Specification Rationale

This section identifies the security functions provided by the TOE mapped to the security functional requirement components contained in this ST. This mapping is provided in the following table.

Security Function	Security Functional Components
Security Audit (FAU)	FAU_GEN.1 Audit data generation
	FAU_SAR.1 Audit review
	FAU_SAR.2 Restricted audit review
	FAU_SAR.3 Selectable audit review
	FAU_SEL.1 Selective audit
	FAU_STG.2 Guarantees of audit data availability
	FAU_STG.4 Prevention of Data Loss
Cryptographic Support (FCS)	FCS_CKM.1 Cryptographic key generation
	FCS_COP.1 Cryptographic operation
Identification and Authentication (FIA)	FIA_UAU.1 Timing of authentication
	FIA_ATD.1 User attribute definition
	FIA_UID.1 Timing of identification
	FIA_AFL.1 Authentication failure handling
	FIA_AFL.1(1) Authentication failure handling
Security Management (FMT)	FMT_MOF.1 Management of security functions behavior
	FMT_MTD.1 Management of TSF data
	FMT_MTD.1(1) Management of TSF data
	FMT_MTD.1(2) Management of TSF data
	FMT_MTD.1(3) Management of TSF data
	FMT_MTD.1(4) Management of TSF data
	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles
Protection of the TSF (FPT)	FPT_STM.1 Reliable time stamps
	FPT_ITA.1 Inter-TSF availability within a defined availability metric
	FPT_ITC.1 Inter-TSF confidentiality during transmission
	FPT_ITI.1 Inter-TSF detection of modification
Intrusion Detection System (IDS)	IDS_SDC.1 System Data Collection
	IDS_ANL.1 Analyzer analysis
	IDS_RCT.1 Analyzer react
	IDS_RDR.1 Restricted Data Review

Security Function	**Security Functional Components**
	IDS_STG.1 Guarantee of System Data Availability
	IDS_STG.2 Prevention of System data loss
Trusted Path/Channel (FTP)	FTP_TRP.1 Trusted Path

Table 9-7: Security Functional Components for the TOE

9.2.1 Security Audit

The audit functions of the TOE enforce the FAU_GEN.1, FAU_SAR.1, FAU_SAR.2, FAU_SEL.1, FAU_STG.2, and FAU_STG.4 requirements.

Section 9.1.1 details how the TOE collects security and system audit information. Only System Administrators are able to view and edit report information about system activity across networks.

The generation of audit data (FAU_GEN.1.1) is provided in Section 2.5.1 of the Introduction, as well as in the section 9.1.1 of the TSS. In addition to the generation of audit data, Section 9.1.1 discusses the specific events that are audited as well as what information is recorded from each record. FAU_GEN.1.2 is further fulfilled in Section 9.1.1 with the mapping of information audited in relation to the event that is occurring. Section 2.5.1 covers the same information, albeit at a high-level.

FAU_SAR.1, FAU_SAR.2, and FAU_SAR.3 are covered in the TSS (Section 9.1.1). This section discusses the privileges users and administrators need to have in order to view the audit data. FAU_SAR.3 is also discussed in Section 9.1.1 where it states that only users with the proper privileges have the ability to sort the audit data. This section demonstrates the use of privileges to apply restrictions on auditing.

FAU_STG.2 is covered in Section 9.1.1 with the discussion of ensuring that the audit data is not able to be modified or deleted by unauthorized users. The TSF, as stated in Section 9.1.1 also ensures that the most recent audit logs are maintained when audit storage has been exhausted. Finally, FAU_STG.4.1 is covered in Section 9.1.1 with the discussion of alarms being sent in the event that the audit trail has reached capacity as well as overwriting the oldest stored audit logs.

Together, the Logical Boundary and TOE Summary Specification sections of the ST satisfy the above listed requirements.

9.2.2 Encrypted Communications

FCS_CKM.1, FCS_COP.1, and FTP_TRP.1 support Encrypted Communications.

Section 2.5.3 states that remote users establish a secure session with the TOE using a browser based GUI. Cryptographic keys are generated for communication with these remote users and between TOE subsystems.

Section 9.1.4 states remote users establish a secure path via OpenSSH v0.9.8b for authentication and TOE management. All encryption and decryption performed by the TOE uses AES in CBC mode with 256-bit keys. All key management performed by the TOE uses RSA with 1024-bit keys.

Together, the Logical Boundary and TOE Summary Specification sections of the ST satisfy the above listed requirements.

9.2.3 Identification and Authentication

The Identification and Authentication function of the TOE enforces the FIA_UAU.1, FIA_ATD.1, FIA_AFL.1, FIA_AFL.1 (1), and FIA_UID.1 requirements.

QRadar uses authentication data and the concept of privileges to determine a user's system access rights and operations capable of being performed.

In the Introduction Section 2.5.2 discusses the basic overview of the identification and authentication requirements and is covered in further detail in the subsequent sections of the TSS, which are discussed below.

Section 9.1.2 discusses the primary attributes for users of the TOE. These attributes serve to assign the proper abilities to users. Information such as user name, authentication data, and CIDR address ranges, devices, device groups, and assigned privileges are used in this determination of how *much* access a user has on the system. This information supports the FIA_ATD.1 requirement.

Contained in the same section, is a discussion on users not being able to perform any actions on the TOE unless they are both identified and authenticated. This information supports the FIA_UAU.1 and FIA_UID.1 requirements.

Together, the Logical Boundary and TOE Summary Specification sections of the ST satisfy the above listed requirements.

9.2.4 Security Management

The security management function of the TOE enforces the FMT_MOF.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1 (4), FMT_SMF.1, and FMT_SMR.1 requirements.

Security Management is required in order to manage the users, the privileges associated with these users, and other data associated with the TOE. This is supporting identification and authentication, security audit, and intrusion detection system requirements.

Section 2.5.3 of the INT provides a general overview of the Security Management requirements as shown above and is further expounded upon in the TSS. The INT, TSS, and SFRs can all be mapped and interpreted through these sections.

The security management requirements as outlined by the TOE are covered by the TSS in Section 9.1.3. The main paragraph of this section identifies the division of roles into Users and Administrators. Before any user account can be created, the role must first be created. Administrators and Users of the TOE have the ability to occupy privileges that have been assigned to them by the primary administrator of the TOE. The discussion of roles clearly supports the FMT_SMR.1 requirement.

In the following sections of the TSS (Section 9.1.3), a lengthy discussion on what specific privileges users and administrators can occupy when given specific privileges and roles. Tables 7-6, 7-7, and 7-8 clearly delineate these abilities that are capable of being performed and who can occupy those roles. This supports the FMT_MTD.1 (1-4) requirements. Furthermore, Section 9.1.3 also states that only authorized System Administrators have the ability to modify system data and the processes that surround it being collected.

Finally, the FMT_SMF.1 is covered by the discussion in Section 9.1.3 that speaks to the TSF being able to perform specific management functions related to auditing, and IDS management.

Together, the Logical Boundary and TOE Summary Specification sections of the ST satisfy the above listed requirements.

9.2.5 Protection of the TSF

The Protection of the TSF function of the TOE enforces the FPT_STM.1, FPT_ITA.1, FPT_ITC.1, and FPT_ITI.1 requirements.

A brief discussion is had regarding the maintaining of reliable date and timestamps for the TOE's processes. The TSS in Section 9.1.4 goes in to further detail of the same topic of maintaining reliable timestamps. This is done so that all TOE subsystems time information is consistent and there are no deviations, and so that system data and audit data records can include the date/time of events.

Section 2.5.4 states TOE administrators ensure that all connections between separate parts of the TOE and between the TOE and trusted third parties are secured using OpenSSH. By providing this level of protection between the TOE and its associated subsystems, a vendor-asserted encrypted solution is maintained.

Section 9.1.5 states that system data is made available to a trusted remote IT product immediately after the TOE's scanning session has been completed. All data transmitted from one TOE subsystem to another is protected from unauthorized disclosure during transmission. The TOE uses secure hashing to detect any modifications unauthorized users have made or attempt to make to protected data. If any modifications have been detected as having occurred, the packet is dropped and the data is requested to be retransmitted.

Together, the Logical Boundary and TOE Summary Specification sections of the ST satisfy the above listed requirements.

9.2.6 Intrusion Detection System

The Intrusion Detection System function of the TOE enforces the IDS_SDC.1, IDS_ANL.1, IDS_RCT.1, IDS_RDR.1, IDS_STG.1, and IDS_STG.2 requirements.

As the primary functionality of an IDS product, these SFRs serve to further enforce the behavior QRadar performs. The TOE is responsible for the collection of, analysis on, and reaction to system data. It uses the data to draw conclusions about whether or not offenses and intrusions have occurred.

Section 2.5.5 of the ST discusses the basic overview of the Intrusion Detection System requirements. These requirements are covered at much greater length in the proceeding sections of the TSS.

Section 9.1.5 states that information is collected from targeted IT system resources which have been defined by the administrator. This statement directly supports the IDS_SDC.1 requirement.

The TSS goes on to speak about what data is analyzed, as well as how it is analyzed by the TOE. The data collected is analyzed to determine if there are any correlations with overall behavior and events. Behavioral and event correlations map directly statistical, signature, and/or integrity data. This is directly applicable to the IDS_ANL.1.1 requirement. Further discussion on the analysis of this data speaks about the data being tagged based on packet header data, threat configuration information, and policy configuration information. This statement directly relates to the IDS_ANL.1.2 requirement.

After analysis has been done, Section 9.1.5 speaks about how intrusions that are detected are reacted to. If an intrusion has been detected, the System send alarms to either the QRadar Console (individuals must have the Offense privilege), the QRadar system log, or email. This pertains to the IDS_RCT.1.1 requirement.

IDS_RDR.1 is covered through the discussion of administrators being provided the ability to read system data and that it should be presented in an easily understandable format (i.e. reports). Only users who have read-access should be able to perform this operation.

Finally, Section 9.1.5 speaks about the guarantee of system data being available. The TOE ensures that system data is protected against unauthorized modification and/or deletion. This enforces the IDS_STG.1.1 and IDS_STG.1.2 requirements. The system also ensures that the most recent system data should be maintained in the event system data storage becomes exhausted. In the event that storage capacity for system data has been reached, the system sends an alarm to the specified individual(s) notifying them of this event.

Together, the Logical Boundary and TOE Summary Specification sections of the ST satisfy the above listed requirements.

10 Security Problem Definition Rationale

10.1 Security Objectives Rationale

The following table provides a mapping with rationale to identify the security environment objectives that address the stated assumptions.

Assumption	Objective	Rationale
A.ACCESS The TOE has access to all the IT System data it needs to perform its functions.	OE.INTROP The TOE is interoperable with the IT System it monitors.	The OE.INTROP objective ensures the TOE has the needed access.
A.DYNMIC The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.	OE.INTROP The TOE is interoperable with the IT System it monitors.	The OE.INTROP objective ensures the TOE has the proper access to the IT System.
	OE.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.	The OE.PERSON objective ensures that the TOE will be managed appropriately.
A.ASCOPE The TOE is appropriately scalable to the IT System the TOE monitors.	OE.INTROP The TOE is interoperable with the IT System it monitors.	The OE.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.
A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.	OE. PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.	The OE.PHYCAL provides for the physical protection of the TOE hardware and software.
A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	OE. PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.	The OE.PHYCAL provides for the physical protection of the TOE.
A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.	OE.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.	The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.
A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.	OE.INSTAL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.	The OE.INSTAL objective ensures that the TOE is properly installed and operated.
	OE. PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.	The OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators.
	OE.CREDEN Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.	The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.

A.NOTRST The TOE can only be accessed by authorized users.	OE. PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.	The OE.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access.
	OE.CREDEN Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.	The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.

Table 10-1: Assumption to Objective Mapping

10.2 Operational Security Policy Rationale

The following table provides a mapping with rationale to identify the security objectives that address the stated Operational Security Policies (OSP).

OSP	Objective	Rationale
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.	O.IDSCAN The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.	The O.IDSCAN objective addresses this policy by requiring collection of Scanner data (IDS_SDC.1).
	O.IDSENS The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.	The O.IDSENS objective addresses this policy by requiring collection of Sensor data (IDS_SDC.1).
	O.AUDITS The TOE must record audit records for data accesses and use of the System functions.	The O.AUDITS objective addresses this policy by requiring collection of audit data (FAU_GEN.1, FAU_SEL.1, FAU_STG.4, ADV_ARC.1, and FPT_STM.1).
	OE.TIME The IT Environment will provide reliable time stamp to the TOE. Time stamps associated with an audit record must be reliable.	The OE.TIME objective addresses this policy by providing reliable time stamps to the TOE (FPT_STM.1).
P.ANALYZ Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.	O.IDANLZ The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).	The O.IDANLZ objective requires analytical processes be applied to data collected from Sensors and Scanners (IDS_ANL.1).

P.MANAGE The TOE shall only be managed by authorized users.	O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.	The O.PROTCT objective addresses this policy by providing TOE self-protection (FAU_STG.2, FMT_MOF.1, FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1 (4), FMT_SMF.1, ADV_ARC.1, and IDS_STG.1).
	O.EADMIN The TOE must include a set of functions that allow effective management of its functions and data.	The O.EADMIN objective ensures there is a set of functions for administrators to use (FAU_SAR.1, FAU_SAR.2, FAU_SEL.1, ADV_ARC.1, and IDS_RCT.1).
	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions (FAU_SAR.2, FAU_STG.2, FIA_UAU.1, FIA_UID.1, FMT_MOF.1, FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1 (4), FMT_SMF.1, IDS_RDR.1, and IDS_STG.1).
	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses (FAU_SAR.2, FAU_STG.2, FIA_UAU.1, FIA_ATD.1, FIA_UID.1, FMT_MOF.1, FMT_MTD.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_SMF.1, FMT_SMR.1, ADV_ARC.1, IDS_RDR.1, IDS_STG.1).
	OE.INSTAL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.	The OE.INSTAL objective supports the OE.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy.
	OE.CREDEN Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.	The OE.CREDEN objective requires administrators to protect all authentication data.

	OE.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.	The OE.PERSON objective ensures competent administrators will manage the TOE.
P.ACCESS All data collected and produced by the TOE shall only be used for authorized purposes.	O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.	The O.PROTCT objective addresses this policy by providing TOE self-protection (FAU_STG.2, FMT_MOF.1, FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1 (4), FMT_SMF.1, ADV_ARC.1, and IDS_STG.1).
	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions (FAU_STG.2, FMT_MOF.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1 (4), FMT_SMF.1, FMT_MTD.1, ADV_ARC.1, and IDS_STG.1).
	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses (FAU_SAR.2, FAU_STG.2, FIA_UAU.1, FIA_ATD.1, FIA_UID.1, FMT_MOF.1, FMT_MTD.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_SMF.1, FMT_SMR.1, ADV_ARC.1, IDS_RDR.1, IDS_STG.1).
	OE.AUDIT_PROTECTION The IT Environment will provide the capability to protect audit information.	The OE.AUDIT_PROTECTION objective addresses this policy by providing audit information protection (FAU_STG.2).
P.ACCACT Users of the TOE shall be accountable for their actions within the IDS.	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated (FAU_SAR.2, FAU_STG.2, FIA_UAU.1, FIA_ATD.1, FIA_UID.1, FMT_MOF.1, FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3),

		FMT_MTD.1 (4), FMT_SMF.1, FMT_SMR.1, ADV_ARC.1, IDS_RDR.1, and IDS_STG.1).
	O.AUDITS The TOE must record audit records for data accesses and use of the System functions.	The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions (FAU_SAR.2, FAU_STG.2, FIA_UAU.1, FIA_ATD.1, FIA_UID.1, FMT_MOF.1, FMT_MTD.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_SMF.1, FMT_SMR.1, ADV_ARC.1, IDS_RDR.1, IDS_STG.1).
	OE.TIME The IT Environment will provide reliable timestamps to the TOE.	The OE.TIME objective addresses this policy by providing reliable time stamps to the TOE (FPT_STM.1).
	OE.AUDIT_SORT The IT Environment will provide the capability to sort the audit information.	The OE.AUDIT_SORT objective addresses this policy by providing audit sorting capabilities (FAU_SAR.3).
P.INTGTY Data collected and produced by the TOE shall be protected from modification.	O.INTEGR The TOE must ensure the integrity of all audit and System data.	The O.INTEGR objective ensures the protection of data from modification (FAU_STG.2, FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1 (4), FPT_ITC.1, FPT_ITI.1, ADV_ARC.1, and IDS_STG.1).
P.PROTCT The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.	O.OFLOWS The TOE must appropriately handle potential audit and System data storage overflows.	The O.OFLOWS objective counters this policy by requiring the TOE handle disruptions (FAU_STG.2, FAU_STG.4, IDS_STG.1, and IDS_STG.2).
	OE. PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.	The OE.PHYCAL objective protects the TOE from unauthorized physical modifications.

Table 10-2: OSP to Objective Mapping

The following table provides a mapping with rationale to identify the security objectives that address the stated threats.

Threat	Objective	Rationale
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.	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	The O.IDAUTH objective provides for authentication of users prior to any TOE data access (FAU_SAR.2, FAU_STG.2, FIA_UAU.1, FIA_ATD.1, FIA_UID.1, FMT_MOF.1, FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1(4), FMT_SMR.1, ADV_ARC.1, IDS_RDR.1, IDS_STG.1, FIA_AFL.1, FIA_AFL.1(1)).
	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data (FAU_SAR.2, FAU_STG.2, FIA_UAU.1, FIA_UID.1, FMT_MOF.1, FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1 (4), FMT_SMF.1, IDS_RDR.1, and IDS_STG.1, FIA_AFL.1, FIA_AFL.1(1)).
	O.INTEGR The TOE must ensure the integrity of all audit and System data.	The O.INTEGR objective ensures no TOE data will be modified (FAU_STG.2, FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1 (4), ADV_ARC.1, IDS_STG.1, FPT_ITC.1, and FPT_ITI.1).
	O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.	The O.PROTCT objective addresses this threat by providing TOE self-protection (FAU_STG.2, FMT_MOF.1, FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1 (4), FMT_SMF.1, ADV_ARC.1, and IDS_STD.1).
T.COMDIS An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	The O.IDAUTH objective provides for authentication of users prior to any TOE data access (FAU_SAR.2, FAU_STG.2, FIA_UAU.1,

Threat	Objective	Rationale
		FIA_ATD.1, FIA_UID.1, FMT_MOF.1, FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1(4), FMT_SMR.1, ADV_ARC.1, IDS_RDR.1, IDS_STG.1, FIA_AFL.1, FIA_AFL.1(1)).
	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data (FAU_SAR.2, FAU_STG.2, FIA_UAU.1, FIA_UID.1, FMT_MOF.1, FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1 (4), FMT_SMF.1, IDS_RDR.1, and IDS_STG.1, FIA_AFL.1, FIA_AFL.1(1)).
	O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.	The O.PROTCT objective addresses this threat by providing TOE self-protection (FAU_STG.2, FMT_MOF.1, FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1 (4), FMT_SMF.1, ADV_ARC.1, and IDS_STD.1).
	O.EXPORT When any IDS component makes its data available to another IDS components, the TOE will ensure the confidentiality of the System data.	The O.EXPORT objective ensures that confidentiality of TOE data will be maintained (FPT_ITA.1, FPT_ITC.1, and FPT_ITI.1).
T.LOSSOF An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	The O.IDAUTH objective provides for authentication of users prior to any TOE data access (FAU_SAR.2, FAU_STG.2, FIA_UAU.1, FIA_ATD.1, FIA_UID.1, FMT_MOF.1, FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1(4), FMT_SMR.1, ADV_ARC.1, IDS_RDR.1, IDS_STG.1, FIA_AFL.1, FIA_AFL.1(1)).

Threat	Objective	Rationale
	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data (FAU_SAR.2, FAU_STG.2, FIA_UAU.1, FIA_UID.1, FMT_MOF.1, FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1 (4), FMT_SMF.1, IDS_RDR.1, and IDS_STG.1, FIA_AFL.1, FIA_AFL.1(1)).
	O.INTEGR The TOE must ensure the integrity of all audit and System data.	The O.INTEGR objective ensures no TOE data will be deleted (FAU_STG.2, FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1 (4), ADV_ARC.1, IDS_STG.1, FPT_ITC.1, FPT_ITI.1).
	O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.	The O.PROTCT objective addresses this threat by providing TOE self-protection (FAU_STG.2, FMT_MOF.1, FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1 (4), FMT_SMF.1, ADV_ARC.1, and IDS_STD.1).
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.	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses (FAU_SAR.2, FAU_STG.2, FIA_UAU.1, FIA_ATD.1, FIA_UID.1, FMT_MOF.1, FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1(4), FMT_SMR.1, ADV_ARC.1, IDS_RDR.1, IDS_STG.1, FIA_AFL.1, FIA_AFL.1(1)).
	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions (FAU_SAR.2, FAU_STG.2, FIA_UAU.1,

Threat	Objective	Rationale
		FIA_UID.1, FMT_MOF.1, FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1 (4), FMT_SMF.1, IDS_RDR.1, and IDS_STG.1, FIA_AFL.1, FIA_AFL.1(1)).
	O.IDSCAN The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.	The O.IDSCAN, O.IDSENS, and O.IDANLZ objectives address this threat by requiring the TOE to collect and analyze System data, which includes attempts to halt the TOE (IDS_SDC.1, IDS_ANL.1.
	O.IDSENS The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.	The O.IDSCAN, O.IDSENS, and O.IDANLZ objectives address this threat by requiring the TOE to collect and analyze System data, which includes attempts to halt the TOE (IDS_SDC.1, IDS_ANL.1.
	O.IDANLZ The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).	The O.IDSCAN, O.IDSENS, and O.IDANLZ objectives address this threat by requiring the TOE to collect and analyze System data, which includes attempts to halt the TOE (IDS_SDC.1, IDS_ANL.1.
T.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses (FAU_SAR.2, FAU_STG.2, FIA_UAU.1, FIA_ATD.1, FIA_UID.1, FMT_MOF.1, FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1(4), FMT_SMR.1, ADV_ARC.1, IDS_RDR.1, IDS_STG.1, FIA_AFL.1, FIA_AFL.1(1)).
	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions (FAU_SAR.2, FAU_STG.2, FIA_UAU.1, FIA_UID.1, FMT_MOF.1, FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3),

Threat	Objective	Rationale
		FMT_MTD.1 (4), FMT_SMF.1, IDS_RDR.1, and IDS_STG.1, FIA_AFL.1, FIA_AFL.1(1)).
	O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.	The O.PROTCT objective addresses this threat by providing TOE self-protection (FAU_STG.2, FMT_MOF.1, FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1 (4), FMT_SMF.1, ADV_ARC.1, and IDS_STD.1).
T.IMPCON An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.	OE.INSTAL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.	The OE.INSTAL objective states the authorized administrators will configure the TOE properly.
	O.EADMIN The TOE must include a set of functions that allow effective management of its functions and data.	The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product (FAU_SAR.1, FAU_SAR.3, FAU_SEL.1, FMT_SMF.1, ADV_ARC.1, and IDS_RDR.1).
	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses (FAU_SAR.2, FAU_STG.2, FIA_UAU.1, FIA_ATD.1, FIA_UID.1, FMT_MOF.1, FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1 (4), FMT_SMR.1, ADV_ARC.1, IDS_RDR.1, and IDS_STG.1).
	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions (FAU_SAR.2, FAU_STG.2, FIA_UAU.1, FIA_UID.1, FMT_MOF.1, FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1 (4), FMT_SMF.1, IDS_RDR.1, and IDS_STG.1).

Threat	Objective	Rationale
T.INFLUX An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.	O.OFLOWS The TOE must appropriately handle potential audit and System data storage overflows.	The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows (FAU_STG.2, FAU_STG.4, IDS_STG.1, and IDS_STG.2).
T.FACCNT Unauthorized attempts to access TOE data or security functions may go undetected.	O.AUDITS The TOE must record audit records for data accesses and use of the System functions.	The O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions (FAU_GEN.1, FAU_SEL.1, FAU_STG.4, FMT_SMF.1, ADV_ARC.1, and FPT_STM.1).
T.SCNCFG Improper security configuration settings may exist in the IT System the TOE monitors.	O.IDSCAN The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.	The O.IDSCAN objective counters this threat by requiring a TOE, which contains a Scanner, collect and store static configuration information that might be indicative of a configuration setting change. The ST will state whether this threat must be addressed by a Scanner (IDS_SDC.1).
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.	O.IDSCAN The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.	The O.IDSCAN objective counters this threat by requiring a TOE, which contains a Scanner, collect and store static configuration information that might be indicative of malicious code. The ST will state whether this threat must be addressed by a Scanner (IDS_SDC.1).
T.SCNVUL Vulnerabilities may exist in the IT System the TOE monitors.	O.IDSCAN The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.	The O.IDSCAN objective counters this threat by requiring a TOE, which contains a Scanner, collect and store static configuration information that might be indicative of vulnerability. The ST will state whether this threat must be addressed by a Scanner (IDS_SDC.1).
T.FALACT The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.	O.RESPON The TOE must respond appropriately to analytical conclusions.	The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity (IDS_RCT.1).

Threat	Objective	Rationale
T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.	O.IDANLZ The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).	The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source (IDS_ANL.1).
T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.	O.IDANLZ The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).	The O. IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources (IDS_ANL.1).
T.MISUSE Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.	O.AUDITS The TOE must record audit records for data accesses and use of the System functions.	The O.AUDITS (FAU_GEN.1, FAU_SEL.1, FAU_STG.4, FMT_SMF.1, ADV_ARC.1, and FPT_STM.1) and O.IDSENS (IDS_SDC.1) objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.
	O.IDSENS The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.	The O.AUDITS (FAU_GEN.1, FAU_SEL.1, FAU_STG.4, FMT_SMF.1, ADV_ARC.1, and FPT_STM.1) and O.IDSENS (IDS_SDC.1) objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.
T.INADVE Inadvertent activity and access may occur on an IT System the TOE monitors.	O.AUDITS The TOE must record audit records for data accesses and use of the System functions.	The O.AUDITS (FAU_GEN.1, FAU_SEL.1, FAU_STG.4, FMT_SMF.1, ADV_ARC.1, and FPT_STM.1) and O.IDSENS (IDS_SDC.1) objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.
	O.IDSENS The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.	The O.AUDITS (FAU_GEN.1, FAU_SEL.1, FAU_STG.4, FMT_SMF.1, ADV_ARC.1, and FPT_STM.1) and O.IDSENS (IDS_SDC.1) objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

Threat	Objective	Rationale
T.MISACT Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.	O.AUDITS The TOE must record audit records for data accesses and use of the System functions.	The O.AUDITS (FAU_GEN.1, FAU_SEL.1, FAU_STG.4, FMT_SMF.1, ADV_ARC.1, and FPT_STM.1) and O.IDSENS (IDS_SDC.1) objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.
	O.IDSENS The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.	The O.AUDITS (FAU_GEN.1, FAU_SEL.1, FAU_STG.4, FMT_SMF.1, ADV_ARC.1, and FPT_STM.1) and O.IDSENS (IDS_SDC.1) objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.
T.EAVESDROPPING A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.	O.EAVESDROPPING The TOE will encrypt TSF data that traverses the network to prevent malicious users from gaining unauthorized access to TOE data.	O.EAVESDROPPING (FCS_CKM.1, FCS_COP.1 FPT_TRP.1, FPT_ITI, FPT_ITC.1) mitigates T.EAVESDROPPING by ensuring that all communication to/from the TOE is not sent unless it is encrypted.
	OE.KEYDESTRUCT The Operational Environment of the TOE is in charge of destroying cryptographic keys when they are no longer necessary.	OE.KEYDESTRUCT mitigates T.EAVESDROPPING and satisfies the FCS_CKM.1 and FCS_COP.1 dependencies on FCS_CKM.4 by asserting that all cryptographic keys will be destroyed by the underlying OS when they are no longer needed.

Table 10-3: Threat to Objective Mapping

10.3 Security Functional Requirements Rationale

The following table provides a mapping with rationale to identify the security functional requirement components that address the stated TOE security objectives.

Objective	Security Functional Components	Rationale
O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data	FAU_STG.2 Guarantees of Audit Data Availability	The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The System is required to protect the
	FMT_MOF.1 Management of Security Functions Behaviour	
	FMT_MTD.1 Management of TSF Data	
	FMT_MTD.1(1) Management of	

Objective	Security Functional Components	Rationale
	TSF Data FMT_MTD.1(2) Management of TSF Data FMT_MTD.1(3) Management of TSF Data FMT_MTD.1(4) Management of TSF Data FMT_SMF.1 Specification of management functions ADV_ARC.1 Architectural Design IDS_STG.1 Guarantee of System Data Availability	System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1 (4)]. The TOE must perform security management and IDS management for auditing, attributes, reports, alerts, and system data [FMT_SMF.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].
O.IDSCAN The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System	IDS_SDC.1 System Data Collection	A System containing a Scanner is required to collect and store static configuration information of an IT System. The type of configuration information collected must be defined in the ST [IDS_SDC.1].
O.EXPORT When any IDS component makes its data available to another IDS components, the TOE will ensure the confidentiality of the System data	FPT_ITA.1 Inter-TSF availability within a defined availability metric FPT_ITC.1 Inter-TSF confidentiality during transmission FPT_ITI.1 Inter-TSF detection of modification	The TOE must make the collected data available to other IT products [FPT_ITA.1]. The TOE must protect all data from modification and ensure its integrity when the data is transmitted to another IT product [FPT_ITC.1, FPT_ITI.1]. The TOE uses the SSH protocol to protect both the confidentiality and integrity of all TSF data that is transmitted between the TSF and any remote trusted IT products. These protections are discussed in RFC 4253 "The Secure Shell (SSH) Transport Layer Protocol." Section 6.3 states that "...the packet length, padding length, payload, and padding fields of each packet MUST be encrypted with the

Objective	Security Functional Components	Rationale
		given algorithm." The payload in this case refers to TSF data and the encryption means that there will be no unauthorized disclosure in accordance with FPT_ITC.1 Inter-TSF confidentiality during transmission. Section 6.4 states that "Data integrity is protected by including with each packet a MAC that is computed from a shared secret, packet sequence number, and the contents of the packet." This means that a message authentication code is included with each packet that is calculated based on the packet contents (i.e. payload or TSF data). Therefore, if TSF data is modified in transit, the MAC will no longer match the packet contents and the modification will be detected in accordance with FPT_ITI.1 Inter-TSF detection of modification. The requirements for FPT_ITC.1 have therefore been satisfied by the TOE.
O.IDSENS The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS	IDS_SDC.1 System Data Collection	A System containing a Sensor is required to collect events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets of an IT System. These events must be defined in the ST [IDS_SDC.1].
O.IDANLZ The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future)	IDS_ANL.1 Analyzer Analysis	The Analyzer is required to perform intrusion analysis and generate conclusions [IDS_ANL.1].
O.RESPON The TOE must respond appropriately to analytical conclusions	IDS_RCT.1 Analyzer React	The TOE is required to respond accordingly in the event an intrusion is detected [IDS_RCT.1].
O.EADMIN The TOE must include a set of functions that allow effective management of its functions and data	FAU_SAR.1 Audit Review FAU_SAR.3 Selectable Audit Review FAU_SEL.1 Selective Audit FMT_SMF.1 Specification of management functions ADV_ARC.1 Architectural Design	The TOE must provide the ability to review and manage the audit trail of the System [FAU_SAR.1, FAU_SEL.1]. The System must provide the ability for authorized administrators to view all System data collected and produced [IDS_RDR.1].

Objective	Security Functional Components	Rationale
	IDS_RDR.1 Restricted Data Review	The TOE must perform security management and IDS management for auditing, attributes, reports, alerts, and system data [FMT_SMF.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].
O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data	FAU_SAR.2 Restricted Audit Review FAU_STG.2 Guarantees of Audit Data Availability FIA_UAU.1 Timing of Authentication FIA_UID.1 Timing of Identification FMT_MOF.1 Management of Security Functions Behaviour FMT_MTD.1 Management of TSF Data FMT_MTD.1(1) Management of TSF Data FMT_MTD.1(2) Management of TSF Data FMT_MTD.1(3) Management of TSF Data FMT_MTD.1(4) Management of TSF Data FMT_SMF.1 Specification of management functions IDS_RDR.1 Restricted Data Review IDS_STG.1 Guarantee of System Data Availability FIA_AFL.1 Authentication Failure Handling FIA_AFL.1(1) Authentication Failure Handling	The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. The TOE must perform security management and IDS management for auditing, attributes, reports, alerts, and system data [FMT_SMF.1]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1 (4),] The TOE does not support external IT products accessing the appliance [FIA_AFL.1]. Users are allowed to attempt to authenticate to the TOE 5 times before being locked out for 30 minutes [FIA_AFL.1(1)].

Objective	Security Functional Components	Rationale
O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data	FAU_SAR.2 Restricted Audit Review	The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. The TOE is required to protect the stored audit logs from unauthorized deletion [FAU_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. Security attributes of subjects use to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1, FMT_MTD.1 (1), FMT_MTD.1 (2), FMT_MTD.1 (3), FMT_MTD.1 (4),]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1]. QRadar does not support external IT products accessing the appliance. [FIA_AFL.1]. Users are allowed to attempt to authenticate to the TOE 5 times before being locked out for 30 minutes [FIA_AFL.1(1)].
	FAU_STG.2 Guarantees of Audit Data Availability	
	FIA_UAU.1 Timing of Authentication	
	FIA_ATD.1 User Attribute Definition	
	FIA_UID.1 Timing of Identification	
	FMT_MOF.1 Management of Security Functions Behaviour	
	FMT_MTD.1 Management of TSF Data	
	FMT_MTD.1(1) Management of TSF Data	
	FMT_MTD.1(2) Management of TSF Data	
	FMT_MTD.1(3) Management of TSF Data	
	FMT_MTD.1(4) Management of TSF Data	
	FMT_SMR.1 Security Roles	
	ADV_ARC.1 Architectural Design	
	IDS_RDR.1 Restricted Data Review	
	IDS_STG.1 Guarantee of System Data Availability	
	FIA_AFL.1 Authentication Failure Handling	
	FIA_AFL.1(1) Authentication Failure Handling	
O.OFLOWS The TOE must appropriately handle potential	FAU_STG.2 Guarantee of Audit Data Availability	The TOE is required to protect the audit data from deletion as well as
	FAU_STG.4 Prevention of Data	

Objective	Security Functional Components	Rationale
audit and System data storage overflows	Loss IDS_STG.1 Guarantee of System Data Availability IDS_STG.2 Prevention of System Data Loss	guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The TOE must prevent the loss of audit data in the event its audit trail is full [FAU_STG.4]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. The System must prevent the loss of audit data in the event its audit trail is full [IDS_STG.2].
O.AUDITS The TOE must record audit records for data accesses and use of the System functions	FAU_GEN.1 Audit Data Generation FAU_SEL.1 Selective Audit FAU_STG.4 Prevention of audit data loss FMT_SMF.1 Specification of management functions ADV_ARC.1 Architectural Design FPT_STM.1 Reliable Time Stamps	Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The TOE must provide the capability to select which security-relevant events to audit [FAU.SEL.1]. The TOE must prevent the loss of collected data in the event its audit trail is full [FAU_STG.4]. The TOE must perform security management and IDS management for auditing, attributes, reports, alerts, and system data [FMT_SMF.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1]. Time stamps associated with an audit log must be reliable [FPT_STM.1].
O.INTEGR The TOE must ensure the integrity of all audit and System data	FAU_STG.2 Guarantee of Audit Data Availability FMT_MTD.1 Management of TSF Data FMT_MTD.1(1) Management of TSF Data FMT_MTD.1(2) Management of TSF Data FMT_MTD.1(3) Management of TSF Data FMT_MTD.1(4) Management of TSF Data ADV_ARC.1 Architectural Design FPT_ITC.1 Inter-TSF confidentiality during	The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.1]. Only authorized administrators of the System may query or add audit and System data [FMT_MTD.1]. The System must protect the collected data from modification and ensure its integrity when the data is transmitted to another

Objective	Security Functional Components	Rationale
	transmission FPT_ITI.1 Inter-TSF detection of modification IDS_STG.1 Guarantee of System Data Availability	IT product [FPT_ITC.1, FPT_ITI.1]. The TOE must ensure that all functions to protect the data are not bypassed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1]. The TOE uses the SSH protocol to protect both the confidentiality and integrity of all TSF data that is transmitted between the TSF and any remote trusted IT products. These protections are discussed in RFC 4253 "The Secure Shell (SSH) Transport Layer Protocol." Section 6.3 states that "...the packet length, padding length, payload, and padding fields of each packet MUST be encrypted with the given algorithm." The payload in this case refers to TSF data and the encryption means that there will be no unauthorized disclosure in accordance with FPT_ITC.1 Inter-TSF confidentiality during transmission. Section 6.4 states that "Data integrity is protected by including with each packet a MAC that is computed from a shared secret, packet sequence number, and the contents of the packet." This means that a message authentication code is included with each packet that is calculated based on the packet contents (i.e. payload or TSF data). Therefore, if TSF data is modified in transit, the MAC will no longer match the packet contents and the modification will be detected in accordance with FPT_ITI.1 Inter-TSF detection of modification. The requirements for FPT_ITC.1 have therefore been satisfied by the TOE.
OE.TIME The IT Environment will provide reliable time stamp to the TOE. Time stamps associated with an audit record must be reliable	FPT_STM.1 Reliable Time Stamps	The IT Environment will provide reliable time stamp to the TOE. Time stamps associated with an audit log must be reliable [FPT_STM.1].
OE.AUDIT_SORT The IT Environment will provide the capability to sort audit information	FAU_SAR.3 Selectable Audit Review	The IT environment must provide the ability to review and manage the audit trail of the System to include sorting the audit data [FAU_SAR.3,].

Objective	Security Functional Components	Rationale
OE.AUDIT_PROTECTION The IT Environment will provide the capability to protect audit information	FAU_STG.2 Guarantee of Audit Data Availability	The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2].
O.EAVESDROPPING The TOE will encrypt TSF data that traverses the network to prevent malicious users from gaining unauthorized access to TOE data	FCS_CKM.1 Cryptographic operation	FCS_CKM.1 states the TSF shall generate 1024 bit keys using RSA for key management.
	FCS_COP.1 Cryptographic operation	FCS_COP.1 states that the TSF uses 256 bit keys using AES in CBC mode for encryption and decryption between components.
	FTP_TRP.1 Trusted Path	FTP_TRP.1 states the TOE shall provide a communication path between the TSF and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure. The TSF shall allow remote users to initiate communication via the trusted path, and it shall require the use of the trusted path for initial user authentication and management of the TOE.
	FPT_ITC.1 Inter-TSF confidentiality during transmission	FPT_ITC.1 states that the TOE shall protect all TSF data transferred to remote trusted IT products. FPT-ITI.1 states that the TOE shall have the capability to detect modification using HMAC-MD5 hashing and be able to take action if modifications are detected. The TOE uses the SSH protocol to protect both the confidentiality and integrity of all TSF data that is transmitted between the TSF and any remote trusted IT products. These protections are discussed in RFC 4253 "The Secure Shell (SSH) Transport Layer Protocol." Section 6.3 states that "...the packet length, padding length, payload, and padding fields of each packet MUST be encrypted with the given algorithm." The payload in this case refers to TSF data and the encryption means that there will be no unauthorized disclosure in accordance with FPT_ITC.1 Inter-TSF confidentiality during transmission.
	FPT_ITI.1 Inter-TSF detection of modification	

Objective	Security Functional Components	Rationale
		Section 6.4 states that "Data integrity is protected by including with each packet a MAC that is computed from a shared secret, packet sequence number, and the contents of the packet." This means that a message authentication code is included with each packet that is calculated based on the packet contents (i.e. payload or TSF data). Therefore, if TSF data is modified in transit, the MAC will no longer match the packet contents and the modification will be detected in accordance with FPT_ITI.1 Inter-TSF detection of modification. The requirements for FPT_ITC.1 have therefore been satisfied by the TOE.

Table 10-4: Security Functional Requirements Rationale

10.4 EAL3 Justification

The threats that were chosen for this ST are consistent with attacker of low attack potential, as specified in the IDS System PP. The IDS System PP is explicitly defined as one for the United States government. EAL3 SARs have been included in this ST in order to provide additional assurance for consumers outside the US which may not acknowledge the SARs presented in the PP as sufficient to ensure basic robustness. The SARs for an EAL3 differ from EAL2 in the areas of development, life-cycle support, and Testing. With EAL3 comes an added focus on supporting and non-interfering actions, error messages, interactions between subsystems of the TSF, evidence to support the usage of a CM plan by a CM system, developers of TSF relevant configuration items, testing of all TSFIs specified in the FSP, coverage testing, and the addition of depth testing.

T.EAVESDROPPING was added as an additional threat above and beyond the threats in the IDS System PP due to the environment posing a higher threat than basic, which is what the IDS System PP specifies. O.EAVESDROPPING was also added to mitigate T.EAVESDROPPING, with the added cryptographic and trusted path requirements mapped to it in order to address the higher threat potential of a malicious user eavesdropping on network traffic to gain unauthorized access to TOE data.

10.5 Requirement Dependency Rationale

The IDS System PP does satisfy all the requirement dependencies of the Common Criteria. The table below lists each requirement from the IDS System PP as well as added SFRs with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Functional Component	Dependency	Included
FAU_GEN.1	FPT_STM.1	YES
FAU_SAR.1	FAU_GEN.1	YES
FAU_SAR.2	FAU_SAR.1	YES
FAU_SAR.3	FAU_SAR.1	YES
FAU_SEL.1	FAU_GEN.1	YES
	FMT_MTD.1	YES
FAU_STG.2	FAU_GEN.1	YES
FAU_STG.4	FAU_STG.2	YES
FIA_UAU.1	FIA_UID.1	YES
FMT_MOF.1	FMT_SMR.1	YES
FMT_MTD.1	FMT_SMR.1	YES
FMT_SMR.1	FIA_UID.1	YES
FCS_CKM.1	FCS_COP.1	YES
	FCS_CKM.4	NO, OE handles this (OE.KEYDESTRUCT)
FCS_COP.1	FCS_CKM.1	YES
	FCS_CKM.4	NO, OE handles this (OE.KEYDESTRUCT)

Table 10-5: Requirement Dependencies

10.6 Strength of Function Rationale

The TOE minimum strength of function is SOF-basic. The evaluated TOE is intended to operate in commercial and DoD low robustness environments processing unclassified information. This security function is in turn consistent with the security objectives described in section 5.

10.7 Assurance Measures

The SARs for this evaluation have been chosen because they are consistent with the package claim of EAL3. Augmentations to this claim include ALC_FLR.2. ALC_FLR.2 provides assurance that the TOE is updated in a well-defined manner that is consistent with the development security procedures outlined in ALC_DVS.1.

The following table identifies the SARs for this ST.

Component	Document(s)	Rationale
ADV_ARC.1 Security Architecture Design	TOE Design Specification Document for Q1 Labs, Inc. QRadar Release 7.0.0 v0.4	This document describes the security architecture of the TOE.
ADV_FSP.3 Functional Specification with complete summary	Functional Specification Document for Q1 Labs, Inc. QRadar Release 7.0.0 v0.4	This document describes the functional specification of the TOE with complete summary.

Component	Document(s)	Rationale
ADV_TDS.2 Architectural Design	TOE Design Specification Document for Q1 Labs, Inc. QRadar Release 7.0.0 v0.4	This document describes the architectural design of the TOE.
AGD_OPE.1 Operational User Guidance	• QRadar Administration Guide r7.0.0 • QRadar Users Guide r7.0.0 • Evaluated Configuration for Q1 Labs QRadar 7.0.0	This document describes the operational user guidance for the TOE.
AGD_PRE.1 Preparative Procedures	• QRadar Administration Guide r7.0.0 • QRadar Users Guide r7.0.0 • Evaluated Configuration for Q1 Labs QRadar 7.0.0	This document describes the preparative procedures that need to be done prior to installing the TOE.
ALC_CMC.3 Authorizations Controls	• Q1 Labs Life Cycle 20101022.doc • Roles in the Product Development Life Cycle.doc	This document describes the authorization controls for the TOE.
ALC_CMS.3 CM Scope	• 6.3.1.143036.toelist.txt • 6.3.1.143036-documentation.toelist.txt • 7.0.0.165643.toelist.txt • 7.0.0.165643-documentation.toelist.txt	These documents describe the CM scope of the TOE.
ALC_DEL.1 Delivery Procedures	QRadar Delivery-20101020.doc	This document describes product delivery for the TOE and a description of all procedures used to ensure objectives are not compromised in the delivery process.
ALC_DVS.1 Identification of Security Measures	• Employee Agreement.doc • Employee Req Offer.xls • Marketing and Product Requirements Document Process.doc • Q1 Acceptable Use Policy.doc • Q1 Audit Vulnerability Scan Policy.doc • Q1 Corporate Security Policy Statement.doc • Q1 Datacenter Authorization Form.doc • Q1 Datacenter Equipment Installation Form.doc • Q1 Datacenter Equipment Removal Form.doc • Q1 Datacenter Policy.doc • Q1 Internal Lab Security	This document provides an identification of security measures for the TOE.

Component	Document(s)	Rationale
	Policy.doc - Q1 Labs Inc Information Security Policy Statement.doc - Q1 Labs Inc Password Policy.doc - Q1 Labs, Inc[1]. Employment Application.doc - Q1 Laptop Desktop Security Policy.doc - Q1 Laptop Security Policy.doc - Q1 Security Awareness.doc - Q1 Virtual Private Network.doc - Q1 Wireless Communication Policy.doc - Q1_Physical_Access.doc - Q1_Termination_Policy.doc	
ALC_FLR.2 Flaw reporting procedures	- Q1 Labs Life Cycle 20101022.doc - Q1 Mtce As-Is Process 20101022.vsd	This document describes the processes taken for flaw remediation for the TOE.
ALC_LCD.1 Life-Cycle Definition	- Q1 Labs Life Cycle 20101022.doc - Q1 Mtce As-Is Process 20101022.vsd	This document provides the life-cycle definition of the TOE.
ASE_CCL.1 Conformance Claims	Q1 Labs QRadar Release 7.0.0 Security Target v1.2	This document describes the CC conformance claims made by the TOE.
ASE_ECD.1 Extended Components Definition	Q1 Labs QRadar Release 7.0.0 Security Target v1.2	This document provides a definition for all extended components in the TOE.
ASE_INT.1 Security Target Introduction	Q1 Labs QRadar Release 7.0.0 Security Target v1.2	This document describes the Introduction of the Security Target.
ASE_OBJ.2 Security Objectives	Q1 Labs QRadar Release 7.0.0 Security Target v1.2	This document describes all of the security objectives for the TOE.
ASE_REQ.2 Security Requirements	Q1 Labs QRadar Release 7.0.0 Security Target v1.2	This document describes all of the security requirements for the TOE.
ASE_SPD.1 Security Problem Definition	Q1 Labs QRadar Release 7.0.0 Security Target v1.2	This document describes the security problem definition of the Security Target.
ASE_TSS.1 TOE Summary Specification	Q1 Labs QRadar Release 7.0.0 Security Target v1.2	This document describes the TSS section of the Security Target.
ATE_COV.2 Analysis of Coverage	- High Level Category Aggregated.pdf	This document provides an analysis of coverage for the

Component	Document(s)	Rationale
	• QRadar Test Case Attachments 20100825.doc • QRadar Test Plan 20100826.doc • Test Result Matrix 20100825.xls	TOE.
ATE_DPT.1 Basic Design	• High Level Category Aggregated.pdf • QRadar Test Case Attachments 20100825.doc • QRadar Test Plan 20100826.doc • Test Result Matrix 20100825.xls	This document describes the basic design of the TOE.
ATE_FUN.1 Functional Tests	• High Level Category Aggregated.pdf • QRadar Test Case Attachments 20100825.doc • QRadar Test Plan 20100826.doc • Test Result Matrix 20100825.xls	This document describes the functional tests for the TOE.
ATE_IND.2 Independent Testing	• Booz_Allen_Q1_QRadar_INDTestProcedures.xlsx • Booz_Allen_Q1_QRadar_INDTestReport.doc	This document describes the independent testing for the TOE.
AVA_VAN.2 Vulnerability Analysis	Booz_Allen_Q1_QRADAR_7.0_VAN_3_20100820.doc	This document describes the vulnerability analysis of the TOE.

Table 10-6: Assurance Requirements Evidence