Trustwave DbProtect Version 6.4.3 Security Target

Version 1.8

July 21, 2015

Trustwave
70 West Madison Street
Suite 1050
Chicago, IL 60602

DOCUMENT INTRODUCTION

Prepared By:

Common Criteria Consulting LLC
15804 Laughlin Lane
Silver Spring, MD 20906
http://www.consulting-cc.com

Prepared For:

Trustwave
70 West Madison Street
Suite 1050
Chicago, IL 60602
http://www.trustwave.com

REVISION HISTORY

Rev	Description
1.0	March 16, 2014, Initial release
1.1	June 24, 2014, Addressed lab ORs/CRs
1.2	July 23, 2014, Addressed certifier ORs/CRs
1.3	October 5, 2014, Consistency with ADV documents, removed audit functionality
1.4	January 17, 2015, Updated user access permissions
1.5	February 9, 2015, Addressed lab ORs
1.6	June 23, 2015, Modified the evaluated platforms and databases
1.7	July 8, 2015, Inserted product build number
1.8	July 21, 2015, Adjusted the database versions supported for scanning

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS LIST

ASE	**Adaptive Server Enterprise**
CC	**Common Criteria**
DAM	**Database Activity Monitoring**
DBMS	**DataBase Management System**
DoS	**Denial of Service**
EAL	**Evaluation Assurance Level**
GUI	**Graphical User Interface**
HTTP	**HyperText Transfer Protocol**
IDS	**Intrusion Detection System**
IIS	**Internet Information Services**
IP	**Internet Protocol**
IT	**Information Technology**
OS	**Operating System**
OSP	**Organisational Security Policy**
PP	**Protection Profile**
RAM	**Random Access Memory**
SFR	**Security Functional Requirement**
SNMP	**Simple Network Management Protocol**
ST	**Security Target**
TOE	**Target of Evaluation**
TSF	**TOE Security Function**

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the Trustwave DbProtect Version 6.4.3. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 3.1*. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

Trustwave DbProtect Version 6.4.3 Security Target, Version 1.8, dated July 21, 2015.

1.2 TOE Reference

Trustwave DbProtect Version 6.4.3 (Build 753)

1.3 Evaluation Assurance Level

Assurance claims conform to EAL2 (Evaluation Assurance Level 2) augmented by ALC_FLR.2 from the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 4.

1.4 TOE Overview

1.4.1 Usage and Major Security Features

The TOE is a database vulnerability assessment and monitoring suite that reports on the security strength of database management systems (also known as database applications) within the network. The TOE helps to identify vulnerable databases residing within the network by scanning for potential security vulnerabilities within those databases and monitoring activity by users with them.

The DbProtect suite is comprised of a web application server (Console) and distributed components for scanning (Scan Engines) and monitoring (Sensors). The users, after they present their credentials to log on to DbProtect (using a web browser) are authenticated against a windows domain or accounts created locally on the web application server. Once logged on, users are authorized to use DbProtect with the privileges granted to them through their assigned roles.

Scan Engines run a defined set of proactive/preventative “jobs” including Discovery jobs that discover databases on the network, Vulnerability Assessment jobs that identify vulnerabilities on the databases, and Rights Management jobs that perform a deep analysis of user and role entitlements on a database.

Vulnerability Assessment consists of a series of security tests or checks that are grouped together in a Policy. Each security test or check targets a specific database application type and performs actions to determine if the application is susceptible to the vulnerability tested for by the check. Checks address:

- Denial of Services—these checks examine the target application for susceptibility to specific Denial of Service (DoS) attacks
- Misconfigurations—these checks examine the target application for possible misconfigurations that may leave the application susceptible to attack

- Password attacks—these checks examine the target application to determine if it is vulnerable to direct password attacks, including: accounts with blank passwords; accounts with default passwords; and susceptibility to dictionary and brute-force attacks
- Vulnerabilities—these checks determine if the application is susceptible to a specific published vulnerability for that application.
- Access Control—these checks examine the target application for potentially inappropriate or insecure access control or privilege settings on database objects
- Application Integrity—these checks determine if specific security measures (such as enabling auditing of specific events or encrypting sensitive data) have been applied in the application
- Identification/Password Control—these checks examine the target application configuration to determine if it might be vulnerable to password attacks or problems associated with user accounts (e.g., by allowing short or poorly constructed passwords).
- OS Integrity—these checks examine aspects of the OS supporting the database application to ensure they do not expose the application to attack (e.g., permissions on database files) and that the database configuration does not introduce vulnerabilities into the OS (e.g., application processes running with elevated privileges)

DbProtect utilizes a library of known vulnerabilities and misconfiguration signatures. DbProtect includes modules that support scanning of the following database management systems (DBMSs): Oracle, Microsoft SQL Server; IBM DB2 LUW; IBM DB2 z/OS; Sybase Adaptive Server Enterprise (ASE); MySQL; Lotus Notes/Domino; and Hadoop.

DbProtect also provides a reactive approach known as Database Activity Monitoring (DAM) to monitor and respond to suspicious database activity. Sensors monitor the actions of privileged users and perform signature matches of suspicious behavior based on custom policies configured for the databases. DbProtect also reacts to configured conditions by generating alerts to users or external systems. Scripts may be invoked to block suspicious or unauthorized activity. Since these scripts depend on actions performed on the database systems (in the Operational Environment), this functionality is not included in the evaluation.

The TOE comprises a single management console component (the Console), one or more database scanning engines (the Scan Engine), and one or more Sensors. Each of these components is an application designed to run in the context of a general purpose operating system. The Console presents the administrative interface, each Scan Engine is responsible for performing the database scanning functions, and each Sensor provides real-time monitoring of database access activities.

The Console is a GUI front-end that centralizes the management of multiple Scan Engines and Sensors, and provides access to the data collected by the Scan Engines and Alerts generated by the Sensors. The Console enables access to set up and run DbProtect jobs. Access to DbProtect functions is role-based and can be limited to specific users based on role assignments within the Console. By assigning users specific roles it is possible to limit access to DbProtect functions and data. Organizations limit the scope of DbProtect scanning and monitoring to a defined set of databases and userids assigned to those Organizations can only run Jobs within the network scope assigned to that Organization.

The product includes a number of supplemental tools that are executed directly from the underlying operating system rather than from the Console, including the Configuration Manager, DbProtect Migration, ASAP Updater, and Policy Editor tools. These tools are not included in the evaluation.

1.5 TOE type

Data Protection

1.6 Required Non-TOE Hardware/Software/Firmware

The TOE consists of applications and services installed on dedicated Windows systems. The following minimum requirements must be satisfied by each system on which a Console or Scan Engine instance is installed.

Table 1 - Server Minimum Requirements

Item	Minimum Requirements
Operating System	Windows Server2012 (64-bit Standard Edition or higher)
Processor	x64 processor at 2.0 GHz, 2 cores
RAM	12GB
Hard Drive	105 MB of free disk space
Networking	One network interface
Web Server (Console only)	IIS
Backend Database	Microsoft SQL Server 2012 (64-bit Standard Edition or higher)
.NET	Microsoft .NET Framework 4.0

Sensor instances are installed on the same system as the database they monitor. For such systems, there are no additional system requirements beyond the system requirements of the database being monitored.

The TOE components store configuration information, scan results, and monitoring results in a single shared backend database instance. The backend database may be collocated with a TOE component or resident on a separate server (in the Operational Environment). System requirements for the system hosting the backend database are dependent on the type of DBMS used.

The Operational Environment provides the database instances to be scanned and monitored by the TOE. The TOE is capable of scanning and monitoring the DBMSs specified in the following table. Requirements for the systems hosting the DBMSs are dependent on the DBMS type. For some DBMS types, additional drivers must be installed on their systems to enable some functions. Specific requirements are provided in the *DbProtect 6.4 Series Getting Started Guide* and *DbProtect 6.4 Series Sensor Guide*.

Table 2 - Supported DBMSs

DBMS	Versions
Oracle (SID)	11gR2, 11gR1
Microsoft SQL Server (Instance)	2012
Sybase ASE (Dataserver)	15.7, 15.5, 15.0
IBM DB2 LUW (Database)	10.1, 9.7, 9.5, 9.1

MySQL (Server)	5.5, 5.1
Hadoop (Node)	1

Users interact with the TOE via remote HTTP sessions with the Console, using Internet Explorer 7 or higher. The remote systems must have JavaScript enabled.

The TOE components depend on Windows to protect their executables and stored data images (e.g., files and registry keys) and their executing environments. The TOE also depends on the environment to ensure the Backend Database is secure. The Operational Environment must protect communication between:

- distributed TOE components (Console, Scan Engines, and Sensors)
- TOE components and the backend database
- Console users and the Console
- Scan Engines and DBMS instances being scanned.

1.7 TOE Description

An operational TOE consists of one instance of the Console, one or more instance of Scan Engines, and one or more instances of Sensors. A single system may host both the Console and Scan Engine.

The TOE allows the authorized administrator to perform the tasks described previously (Discovery, Pen Tests, Audits) as well as examining scan and monitoring results, based on function privileges.

Logically, the Scan Engine operates as a single application though it is instantiated in a series of processes utilizing inter-process communication mechanisms provided by Windows to communicate with one another. Within the host, the Scan Engine executes using the host user credentials it is configured to use.

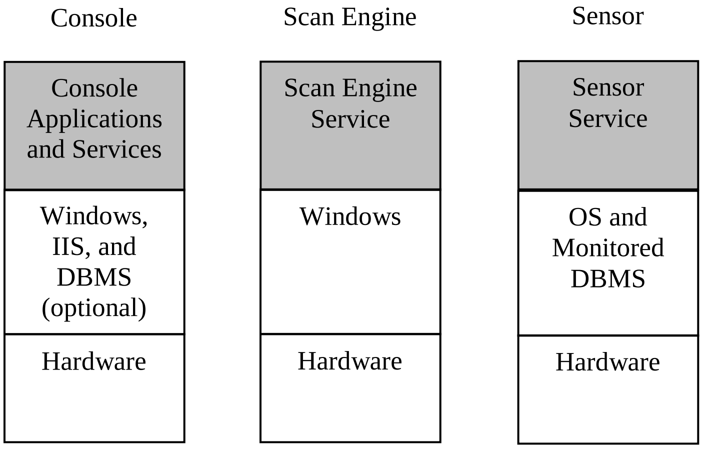
Logically, the Sensor operates as a single application though it is instantiated in a series of processes utilizing inter-process communication mechanisms provided by the host OS to communicate with one another. Within the host, the Sensor executes using the host user credentials it is configured to use.

The Console provides a means of centrally managing multiple Scan Engine and Sensor instances. It implements a Graphical User Interface for the users to manage the TOE. Through the Console, users can access the functions and scan and monitoring results of the Scan Engine and Sensor instances to which they have been granted access.

1.7.1 Physical Boundary

The physical boundary of the TOE includes the Console and Scan Engine applications and services executing on dedicated Windows systems, as well as Sensors executing on the same platforms as DBMS instances being monitored. The operating systems and DBMSs are not included in the TOE boundary.

Figure 1 - Physical Boundary



The physical boundary also includes the following guidance documentation:

1. *Trustwave DbProtect 6.4 Series User Guide*
2. *Trustwave DbProtect 6.4 Series Sensor Guide*
3. *Trustwave DbProtect 6.4.3 Getting Started Guide*
4. *Trustwave DbProtect 6.4 Series Common Criteria Supplement*

1.7.2 Logical Boundary

1.7.2.1 Database Discovery, Scanning, and Monitoring

The TOE discovers, scans, and monitors databases for vulnerabilities and suspicious behavior. Scans are performed to proactively detect vulnerabilities, misconfigurations, and inappropriate permission settings. Monitoring is performed to react to unusual or suspicious behavior. Alerts may be generated for configured conditions.

1.7.2.2 Database Review

Scan and monitoring results can be viewed via the Console. The TOE can also generate reports that identify specific potential vulnerabilities, provide an assessment of the risk associated with a vulnerability, and recommend actions to address vulnerabilities.

1.7.2.3 Identification

The Console requires each user that connects to the Console via a browser session to provide a username and password before he/she can access any Console security functions. The Console passes the provided credentials to Windows for authentication. Access is denied if credential validation fails or the supplied username is not configured as a valid user of the TOE. Upon success, the user attributes are bound to the session.

1.7.2.4 Management

The Console provides security management functions that are accessible via a web browser on remote systems. The Console implements role-based access control features. As such, the Console restricts user access to the management functions.

Two types of roles may be associated with users: system roles and organizational roles. User accounts do not have to be assigned roles of both types.

System roles define the access rights to the management of system-level entities: Scan Engines, Sensors, Organization structure, and Users. Administrator role grants full access to all system-level privileges. Auditor role grants read-only access to all system-level entities. Org Owner role, used in conjunction with an Owner role for an Organization, permits creation of descendent organizations.

Users can be assigned organizational roles, which determine access rights to entities within the associated Organization, as well as any subordinate Organizations. Users have no access rights to Organizations without associated organizational roles. The organizational roles associated with Organizations are Owner, Job Manager, Credential Managers, DataViewers, Asset Managers, and Auditors. The purpose of the organizational roles is to restrict data stored, collected, and associated with an organization to users in that organization.

1.7.3 TSF Data

The following table describes the TSF data used in the TOE.

Table 3 - TSF Data Descriptions

TSF Data	Description
Assets	Define attributes of DBMSs to be scanned. Attributes include: • Name • Assigned Organization • Associated Scan Engine • Identity (IP Address/Hostname, Port, and Instance) • Type • Host OS
Credential Profiles	Define credential sets to be used during scans of Assets. Attributes include: • Name • Type (DBMS or OS) • Username • Password
Filters	Define additional activity to audit while monitoring databases or exceptions to generating Alerts for specific conditions. Attributes include: • Name • Applicable database type • For audited activities, the specific accesses that are audited • For exceptions, the excluded conditional values
Jobs	Define attributes for discovery and scan of Assets. Attributes include: • Name • Organization • Assets • Credential Profiles • Policies • Schedule

TSF Data	Description
Monitoring Policies	Define specific monitoring actions to be performed. Attributes include: • Name • Selected security checks (activity to be monitored) • Applicable database types • Alert level associated with each security check • Assigned exceptions (Filters) for each security check
Organizations	Defines a grouping of other TSF data within the TOE to restrict access for authorized users. Attributes include: • Name • Hierarchy (parent)
Policies	Define specific scan actions to be performed. Attributes include: • Name • Included Controls (items to be checked in scans) • Alert Conditions
Reports	Define reports generated from scan results of scans. Attributes include: • Name • Associated Organization • Information included
Scan Engines	Define the Scan Engines associated with the Console. Attributes include: • Name • IP Address
Scan Results	Collection of results learned from scans and/or monitoring.
Sensors	Define the Sensors associated with the Console. Attributes include: • Name • IP Address • Associated Database • Assigned Monitoring Policies • Alert level
Users	Define attributes for authorized users of the Console. Attributes include: • Username • Set of system and/or organizational roles

1.8 Evaluated Configuration

The evaluated configuration consists of the following TOE components, executing on systems complying with the minimum hardware and software requirements specified for each component:

1. One or more instances of Scan Engines
2. One or more instances of Sensors
3. One instance of the Console

Note that Console and Scan Engine instances may be installed on a single system.

In addition, the following configuration options must be specified to conform to the evaluated configuration:

1. ASAP Update must not be used, since it could result in installation of an unevaluated version of the product.
2. If Sensors are installed, they are installed on the same system as the database they monitor.
3. Usage of the Advanced Filter Editor for monitoring Filters is not included in the evaluation. Filters may be configured using the built-in functions provided by the supplied wizards.
4. The backend database is installed on a stand-alone system or collocated with the Console system.

1.9 Functionality Supported But Not Evaluated

In addition to Windows Server 2012, Windows Server 2008 is also supported as a host platform for the TOE.

In addition to Microsoft SQL Server 2012, Microsoft SQL Server 2008 is also supported as the backend database.

In addition to the databases listed in Table 2, the following database versions are supported for scanning:

- Oracle (SID) - 10gR2, 10gR1, 9iR2
- Microsoft SQL Server (Instance) - 2008 R2, 2008, 2005, 2000
- Sybase ASE (Dataserver) - 12.5
- IBM DB2 LUW (Database) - 10.1
- IBM DB2 z/OS (Subsystem) - 10.1, 9.1, 8.1
- Hadoop (Node) - 2

2. Conformance Claims

2.1 Common Criteria Conformance

Common Criteria version: Version 3.1 Revision 4, dated September 2012

Common Criteria conformance: Part 2 extended and Part 3 conformant

2.2 Security Requirement Package Conformance

EAL2 augmented by ALC_FLR.2

The TOE does not claim conformance to any security functional requirement packages.

2.3 Protection Profile Conformance

The TOE does not claim conformance to any registered Protection Profile.

3. Security Problem Definition

3.1 Introduction

This chapter defines the nature and scope of the security needs to be addressed by the TOE. Specifically this chapter identifies:

A) assumptions about the environment,

B) threats to the assets and

C) organisational security policies.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.2 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE environment. These assumptions may include practical realities in the development of the TOE security requirements and/or the essential environmental conditions on the use of the TOE.

Table 4 - Assumptions

A.Type	Description
A.ACCESS	The TOE has access to all the database 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 database the TOE monitors.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical and logical access.
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.

3.3 Threats

The threats identified in the following subsections are addressed by the TOE and/or the Operational Environment.

Table 5 - Threats

T.Type	Description
T.COMDIS	An unauthorized user may attempt to disclose the data collected by the TOE by bypassing a TOE security mechanism.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected by the TOE by bypassing a security mechanism.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential vulnerability to go undetected.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the collection functionality by halting execution of the TOE.
T.SCNCFG	Improper security configuration settings may exist in the databases the TOE monitors that enable authorized or unauthorized users to gain unauthorized access to data.

T.Type	Description
T.SCNVUL	Vulnerabilities may exist in the databases the TOE monitors that enable authorized or unauthorized users to gain unauthorized access to data.

3.4 Organisational Security Policies

The organisational security policies (OSPs) identified in the following table are addressed by the TOE and/or the Operational Environment.

Table 6 - Organisational Security Policies

P.Type	Description
P.DETECT	Configuration and vulnerability information that might be indicative of the potential for a future intrusion of a targeted IT system (database) must be collected.
P.MANAGE	The TOE shall only be managed by authorized users.

4. Security Objectives

This section identifies the security objectives of the TOE and the TOE's Operational Environment. The security objectives identify the responsibilities of the TOE and the TOE's Operational Environment in meeting the security needs. Objectives of the TOE are identified as *O.objective*. Objectives that apply to the operational environment are designated as *OE.objective*.

4.1 Security Objectives for the TOE

The TOE must satisfy the following objectives.

Table 7 - Security Objectives for the TOE

O.Type	Description
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.IDACTS	The TOE must collect and store configuration and vulnerability information that might be indicative of the potential for a future intrusion of a database.
O.IDENT	The TOE must be able to identify users prior to allowing access to the TOE.
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data via its own interfaces.

4.2 Security Objectives for the Operational Environment

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

Table 8 - Security Objectives of the Operational Environment

OE.Type	Description
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.IDAUTH	The operational environment of the TOE authenticates users prior to allowing access to TOE via its own interfaces.
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 the TOE guidance.
OE.INTROP	The TOE is interoperable with the databases it monitors and scans.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE.
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.PROTECT	The operational environment of the TOE must protect the TOE from logical attacks including unauthorized modifications and access to stored data or TOE executables.
OE.TRANSMIT	The operational environment must protect the data transmitted between the TOE components and the operational environment components.

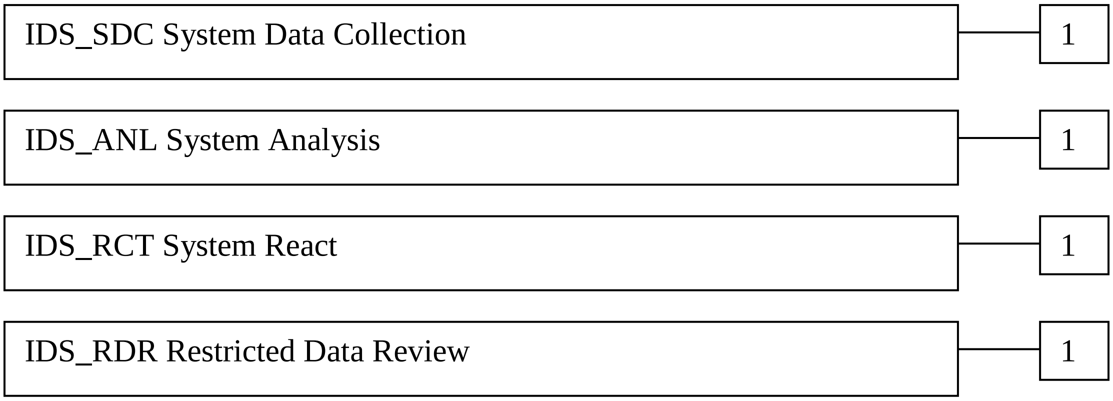
5. Extended Components Definition

5.1 Extended Security Functional Components

5.2 Class IDS: Intrusion Detection

All of the components in this section are based on the U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments.

This class of requirements is taken from the IDS System PP to specifically address the data processed by an IDS System. The audit class of the CC (FAU) was used as a model for creating these requirements. The purpose of this class of requirements is to address the unique nature of system data and provide for requirements about analyzing, reviewing and managing the data.


IDS_SDC System Data Collection
1
IDS_ANL System Analysis
1
IDS_RCT System React
1
IDS_RDR Restricted Data Review
1

5.2.1 IDS_SDC System Data Collection

Family Behaviour:

This family defines the requirements for the TOE regarding collection of information related to security events.

Component Levelling:

IDS_SDC System Data Collection
1

IDS_SDC.1 System Data Collection provides for the functionality to require TSF controlled processing of data for database instances. The data may include database instance identification parameters (e.g. IP address), access control configuration (what user roles or permissions grant access to what data), authentication configuration (how user authentication is performed), accountability policy configuration (what audit records are generated), and user rights assignments (what roles or permissions are assigned to individual users).

Management:

The following actions could be considered for the management functions in FMT:

a) Management of the configuration information related to data collection.

Audit:

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Basic: Processing of log (batch) files.

IDS_SDC.1 System Data Collection

Hierarchical to: No other components.

Dependencies: None

IDS_SDC.1.1 The TSF shall be able to collect and store the following information for database instances: [assignment: *data items collected*].

5.2.2 IDS_ANL System Analysis

Family Behaviour:

This family defines the requirements for the TOE regarding analysis of collected security events.

Component Levelling:

IDS_ANL System Analysis
1

IDS_ANL.1 System Analysis provides for the functionality to require TSF controlled analysis of collected data.

Management:

The following actions could be considered for the management functions in FMT:

a) Configuration of the analysis to be performed.

Audit:

There are no auditable events foreseen.

IDS_ANL.1 System Analysis

Hierarchical to: No other components.

Dependencies: IDS_SDC.1 System Data Collection

IDS_ANL.1.1 The TSF shall perform the following analysis function(s) on all collected security information:

a) [selection: *statistical, signature, integrity*]; and

b) [assignment: *other analytical functions*].

IDS_ANL.1.2 The TSF 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) [assignment: *other security relevant information about the result*].

5.2.3 IDS_RCT System React

Family Behaviour:

This family defines the requirements for the TOE regarding reactions to the analysis of information related to security events.

Component Levelling:

IDS_RCT.1 System React provides for the functionality to require TSF controlled reaction to the analysis of collected data and/or database activity.

Management:

The following actions could be considered for the management functions in FMT:

a) the management (addition, removal, or modification) of actions.

Audit:

There are no auditable events foreseen.

IDS_RCT.1 System React

Hierarchical to: No other components.

Dependencies: IDS_ANL.1 System Analysis

IDS_RCT.1.1 The TSF shall send an alarm to [assignment: *alarm destination*] and take [assignment: *appropriate actions*] when a configured condition is detected.

Application Note: There must be an alarm, though the ST should refine the nature of the alarm and define its target (e.g., administrator console, audit log). The TSF may optionally perform other actions; these actions should be defined in the ST.

5.2.4 IDS_RDR Restricted Data Review

Family Behaviour:

This family defines the requirements for the TOE regarding review of the System data collected by the TOE. System data refers to the set of collected security event information together with the records generated from the analysis of the security event information.

Component Levelling:

IDS_RDR.1 Restricted Data Review provides for the functionality to require TSF controlled review of the System data collected by the TOE.

Management:

The following actions could be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of the group of users with read access right to the System data records.

Audit:

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Basic: Attempts to read System data that are denied.

b) Detailed: Reading of information from the System data records.

IDS_RDR.1 Restricted Data Review

Hierarchical to: No other components.

Dependencies: IDS_ANL.1 System Analysis

IDS_RDR.1.1 The TSF shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of System data*] from the System data.

IDS_RDR.1.2 The TSF shall provide the System data in a manner suitable for the user to interpret the information.

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

5.3 Extended Security Assurance Components

None

6. Security Requirements

This section contains the functional requirements that are provided by the TOE. These requirements consist of functional components from Part 2 of the CC.

The CC defines operations on security requirements. The font conventions listed below state the conventions used in this ST to identify the operations.

Assignment: indicated in italics

Selection: indicated in underlined text

Assignments within selections: indicated in italics and underlined text

Refinement: indicated with bold text

Iterations of security functional requirements may be included. If so, iterations are specified at the component level and all elements of the component are repeated. Iterations are identified by numbers in parentheses following the component or element (e.g., FAU_ARP.1(1)).

6.1 TOE Security Functional Requirements

The functional requirements are described in detail in the following subsections. Additionally, these requirements are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation* with the exception of completed operations.

6.1.1 Identification and Authentication (FIA)

6.1.1.1 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: *UserID, Role, Organization*.

6.1.1.2 FIA_UID.2 User Identification Before any Action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.2 Security Management (FMT)

6.1.2.1 FMT_MTD.1 Management of TSF Data (System-level)

FMT_MTD.1.1(1) The TSF shall restrict the ability to query, modify, delete, *and create* the *system-level data listed in the following table* to *the system-level roles as specified in the following table*.

Table 9 - System-Level TSF Data Permissions

TSF Data	Administrator	Auditor	Org Owner
Monitoring Policies	Query	None	None
Organizations	Query, Modify, Delete, Create	Query	Query, Create subordinate Organization if also Owner of the parent
Scan Engines	Query, Modify, Delete, Create	Query	None
Sensors	Query	None	None
Users	Query, Modify, Delete, Create	Query	Query Modify Organization Roles for users in owned Organizations

Application Note: If multiple system roles are assigned, the permissions granted are the union of the permissions for all of the assigned roles.

6.1.2.2 FMT_MTD.1 Management of TSF Data (Organization-level)

FMT_MTD.1.1(2) The TSF shall restrict the ability to query, modify, delete, *assign and create* the *organization-level data listed in the following table* to *the organization-level roles as specified in the following table*.

Table 10 - Organization-Level TSF Data Permissions

TSF Data	Owner	Job Manager	Credential Manager	Data Viewer	Asset Manager	Auditor
Assets	Query, Create, Modify, Delete, Assign	Query, Assign	Query	Query	Query, Create, Modify, Delete	Query
Credential Profiles	Query, Create, Modify, Delete	Query, Create, Modify, Delete, Assign	Query, Create, Modify, Delete	None	None	Query
Filters	Query, Create, Modify, Delete, Assign	None	None	None	None	Query
Jobs	Query, Create, Modify, Delete	Query, Create, Modify, Delete	None	None	None	Query
Monitoring Policies	Query, Create, Modify, Delete	None	None	Query	None	Query
Organizations (Subordinate)	Query, Modify, Delete Create if also Org Owner system role	Query	Query	Query	Query	Query
Policies	Query, Modify, Delete	Assign	Query	Query	Query	Query
Reports	Query, Create, Modify, Delete	None	None	Query	None	Query
Scan Results	Query, Create, Modify, Delete	Create	None	Query	None	Query
Users	Modify Organizational Roles within the Owner's Organization	None	None	None	None	None

Application Note: System-level Administrators are implicitly the Owners of all top-level Organizations.

Application Note: If multiple roles within an Organization are assigned, the permissions granted within that Organization are the union of the permissions for all of the assigned organizational roles.

6.1.2.3 FMT_SMF.1 Specification of Management Functions

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

- *management of Assets,*
- *management of Jobs,*
- *management of Credential Profiles,*
- *management of Reports,*
- *management of Scan Engines,*
- *management of Sensors,*
- *management of Organizations, and*
- *management of Users.*

6.1.2.4 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles

1. *For System-level permissions:*
   - *a) Administrator*
   - *b) Auditor*
   - *c) Org Owner*
2. *For Organization-level permissions:*
   - *a) Owner*
   - *b) Job Manager*
   - *c) Credential Manager*
   - *d) Data Viewer*
   - *e) Asset Manager*
   - *f) Auditor.*

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

6.1.3 Intrusion Detection (IDS)

6.1.3.1 IDS_SDC.1 System Data Collection

IDS_SDC.1.1 The TSF shall be able to collect and store the following information for database instances: *Name, IP Address or Hostname, Port, Type, Host Operating System, Access Control Configuration, Authentication Configuration, Accountability Policy Configuration, User Rights assignments.*

6.1.3.2 IDS_ANL.1 System Analysis

IDS_ANL.1.1 The TSF shall perform the following analysis function(s) on all collected security information:

a) signature; and

b) *misconfiguration, inappropriate rights assignments, and detected known vulnerabilities.*

IDS_ANL.1.2 The TSF 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) *Matching signature, configuration information*.

6.1.3.3 IDS_RCT.1 System React

IDS_RCT.1.1 The TSF shall send an alarm to *the Console* and take *the following optional actions if configured: send a Syslog, send an SNMP Trap, send an email* when a configured condition is detected.

6.1.3.4 IDS_RDR.1 Restricted Data Review

IDS_RDR.1.1 The TSF shall provide *authorised users* with the capability to read *System data for the Organization they are assigned to as well as all subordinate Organizations* from the System data.

Application Note: Authorized users for specific types of System data.

IDS_RDR.1.2 The TSF shall provide the System data in a manner suitable for the user to interpret the information.

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

6.2 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL2 augmented by ALC_FLR.2. These requirements are summarised in the following table.

Table 11 - EAL2+ Assurance Requirements

Assurance Class	Component ID	Component Title
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

6.3 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 12 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FIA_ATD.1	No other components.	None	n/a
FIA_UID.2	FIA_UID.1	None	n/a
FMT_MTD.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No other components.	None	n/a
FMT_SMR.1	No other components.	FIA_UID.1	Satisfied by FIA_UID.2
IDS_SDC.1	No other components.	None	n/a
IDS_ANL.1	No other components.	IDS_SDC.1	Satisfied
IDS_RCT.1	No other components.	IDS_ANL.1	Satisfied
IDS_RDR.1	No other components.	IDS_ANL.1	Satisfied

7. TOE Summary Specification

7.1 Database Discovery, Scanning, and Monitoring

The TOE is able to discover databases; they may also be manually configured. Scanning is performed against the configured databases to detect known vulnerabilities, misconfiguration, and inappropriate rights assignments (IDS_SDC.1). Information gathered about the databases and activity involving the databases is analyzed (IDS_ANL.1), and configured conditions cause alerts to be generated (IDS_RCT.1).

7.2 Database Review

The TOE provides authorized users with the ability to read information learned about databases in a human readable form via the Console. The information is presented through GUI interactions and Reports (IDS_RDR.1).

7.3 Identification

The TOE performs identification for all access to the Console before granting any other access. When identification is required, the user must enter a username and password. When the credentials are submitted, they are forwarded to Windows for validation. If the credentials are not valid, then the user is notified via a text message and is prompted for credentials again. The TOE also verifies the supplied username against its store of defined accounts (FIA_UID.2). If the credentials are not valid, the user is notified via a text message and is again prompted for credentials. When valid credentials are entered for a defined account, the user attributes (FIA_ATD.1) are bound to the session so that appropriate privileges may be enforced. The TOE supports multiple simultaneous management sessions and tracks the attributes for each session individually.

7.4 Management

The TOE provides management capability to enable the TOE to be controlled and monitored via the Console. The user roles (system-level and organization-level) provide different privileges to accommodate different user roles in an operational environment. The specific privileges for management functions associated with each role are defined in the tables following FMT_MTD.1(1) and FMT_MTD.1(2). The management functions and roles are defined in FMT_SMF.1 and FMR_SMR.1 respectively.

8. Protection Profile Claims

This chapter provides detailed information in reference to the Protection Profile conformance identification that appears in Chapter 2.

8.1 Protection Profile Reference

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

8.2 Protection Profile Refinements

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

8.3 Protection Profile Additions

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

8.4 Protection Profile Rationale

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

9. Rationale

This chapter provides the rationale for the selection of the IT security requirements, objectives, assumptions and threats. It shows that the IT security requirements are suitable to meet the security objectives, Security Requirements, and TOE security functionality.

9.1 Rationale for IT Security Objectives

This section of the ST demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each OSP, threat and assumption is addressed by a security objective.

The following table identifies for each threat and assumption, the security objective(s) that address it.

Table 13 - OSPs, Threats and Assumptions to Security Objectives Mapping

O/T/A Objective	P.DETECT	P.MANAGE	T.COMDIS	T.COMINT	T.IMPCON	T.LOSSOF	T.NOHALT	T.SCNCFG	T.SCNVUL	A.ACCESS	A.DYNMIC	A.LOCATE	A.MANAGE	A.NOEVIL
O.ACCESS		X	X	X	X	X	X	X	X					
O.EADMIN		X												
O.IDACTS	X							X	X					
O.IDENT		X	X	X	X	X	X							
O.PROTCT		X	X	X		X								
OE.CREDEN		X												X
OE.IDAUTH		X	X	X	X	X	X							
OE.INSTAL		X			X									X
OE.INTROP										X	X			
OE.PERSON		X									X		X	
OE.PHYCAL												X		
OE.PROTECT						X	X					X		
OE.TRANSMIT			X	X										

9.1.1 Rationale Showing Threats to Security Objectives

The following table describes the rationale for the threat to security objectives mapping.

Table 14 - Threats to Security Objectives Rationale

T.TYPE	Rationale
T.COMDIS	This Threat is satisfied by ensuring that: • O.ACCESS: The O.ACCESS objective builds upon the OE.IDAUTH objective by only permitting authorized users to access TOE data. • O.IDENT: The O.IDENT objective provides identification of users prior to any TOE function accesses. • OE.IDAUTH: The OE.IDAUTH environment objective in conjunction with O.IDENT provides authentication of users prior to any TOE access. • O.PROTCT: The O.PROTCT objective addresses this threat by providing TOE self-protection. • OE.TRANSMIT: The operational environment must protect the data transmitted between the TOE and operational environment components.
T.COMINT	This Threat is satisfied by ensuring that: • O.ACCESS: The O.ACCESS objective builds upon the OE.IDAUTH objective by only permitting authorized users to access TOE data. • O.IDENT: The O.IDENT objective provides identification of users prior to any TOE function accesses. • OE.IDAUTH: The OE.IDAUTH environment objective in conjunction with O.IDENT provides authentication of users prior to any TOE access. • O.PROTCT: The O.PROTCT objective addresses this threat by providing TOE self-protection. • OE.TRANSMIT: The operational environment must protect the data in transmit between the TOE and operational environment components.
T.IMPCON	This Threat is satisfied by ensuring that: • O.ACCESS: The O.ACCESS objective builds upon the OE.IDAUTH objective by only permitting authorized users to access TOE functions and data. • O.IDENT: The O.IDENT objective provides identification of users prior to any TOE function accesses. • OE.IDAUTH: The OE.IDAUTH environment objective in conjunction with O.IDENT provides authentication of users prior to any TOE access. • OE.INSTAL: The OE.INSTAL objective states the authorized administrators will configure the TOE properly.
T.LOSSOF	This Threat is satisfied by ensuring that: • O.ACCESS: The O.ACCESS objective builds upon the OE.IDAUTH objective by only permitting authorized users to access TOE data. • O.IDENT: The O.IDENT objective provides identification of users prior to any TOE function accesses. • OE.IDAUTH: The OE.IDAUTH environment objective in conjunction with O.IDENT provides authentication of users prior to any TOE access. • O.PROTCT: The O.PROTCT objective addresses this threat by providing TOE self-protection. • OE.PROTECT: The OE.PROTECT objective ensures that the environment provides protection for the TOE data from mechanisms outside of the TOE.

T.TYPE	Rationale
T.NOHALT	This Threat is satisfied by ensuring that: • O.ACCESS: The O.ACCESS objective builds upon the OE.IDAUTH objective by only permitting authorized users to access. • O.IDENT: The O.IDENT objective provides identification of users prior to any TOE function accesses. • OE.IDAUTH: The OE.IDAUTH environment objective in conjunction with O.IDENT provides authentication of users prior to any TOE access. • OE.PROTECT: The OE.PROTECT objective ensures that the environment provides a secure environment for the TOE.
T.SCNCFG	This Threat is satisfied by ensuring that: • O.ACCESS: The O.ACCESS objective builds on O.IDACTS by requiring the results of the scans to be accessible. • O.IDACTS: The O.IDACTS objective counters this threat by requiring the TOE collect and store vulnerability information that might be indicative of a configuration setting change.
T.SCNVUL	This Threat is satisfied by ensuring that: • O.ACCESS: The O.ACCESS objective builds on O.IDACTS by requiring the results of the scans to be accessible. • O.IDACTS: The O.IDACTS objective counters this threat by requiring the TOE collect and store configuration and vulnerability information that might be indicative of a vulnerability.

9.1.2 Rationale Showing Assumptions to Security Objectives

The following table describes the rationale for the assumption to security objectives mapping.

Table 15 - Assumptions to Security Objectives Rationale

A.TYPE	Rationale
A.ACCESS	This Assumption is satisfied by ensuring that: • OE.INTROP: The OE.INTROP objective ensures the TOE has the needed access.
A.DYNMIC	This Assumption is satisfied by ensuring that: • OE.INTROP: The OE.INTROP objective ensures the TOE has the proper access to the database. • OE.PERSON: The OE.PERSON objective ensures that the TOE will be managed appropriately.
A.LOCATE	This Assumption is satisfied by ensuring that: • OE.PHYCAL: The OE.PHYCAL provides for the physical protection of the TOE. • OE.PROTECT: The OE.PROTECT objective ensures that the environment provides protection from logical attacks.
A.MANAGE	This Assumption is satisfied by ensuring that: • OE.PERSON: The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.
A.NOEVIL	This Assumption is satisfied by ensuring that: • OE.CREDEN: The OE.CREDEN objective supports this assumption by requiring protection of all authentication data. • OE.INSTAL: The OE.INSTAL objective ensures that the TOE is properly installed and operated.

9.1.3 Rationale Showing OSPs to Security Objectives

The following table describes the rationale for the OSP to security objectives mapping.

Table 16 - OSPs to Security Objectives Rationale

P.TYPE	Rationale
P.DETECT	This OSP is satisfied by ensuring that: • O.IDACTS: The O.IDACTS objective addresses this policy by requiring collection of scanned configuration and vulnerability data.
P.MANAGE	This OSP is satisfied by ensuring that: • O.ACCESS: The O.ACCESS objective builds upon the O.IDENT and OE.IDAUTH objectives by only permitting authorized users to access TOE functions. • O.EADMIN: the O.EADMIN objective ensures there is a set of functions for administrators to use. • O.IDENT: The O.IDENT objective provides identification of users prior to any TOE function accesses. • OE.IDAUTH: The OE.IDAUTH environment objective in conjunction with O.IDENT provides authentication of users prior to any TOE access. • O.PROTCT: O.PROTCT objective addresses this policy by providing TOE self-protection. • OE.CREDEN: The OE.CREDEN objective requires administrators to protect all authentication data. • OE.INSTAL: The OE.INSTAL objective supports the O.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. • OE.PERSON: The OE.PERSON objective ensures competent administrators will manage the TOE.

9.2 Security Requirements Rationale

9.2.1 Rationale for Security Functional Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

The following table identifies for each TOE security objective and the SFR(s) that address it.

Table 17 - SFRs to Security Objectives Mapping

	O.ACCESS	O.EADMIN	O.IDACTS	O.IDENT	O.PROTCT
FIA_ATD.1				X	
FIA_UID.2				X	
FMT_MTD.1(1)	X				X

	O.ACCESS	O.EADMIN	O.IDACTS	O.IDENT	O.PROTCT
FMT_MTD.1(2)	X				X
FMT_SMF.1		X			
FMT_SMR.1	X				
IDS_SDC.1			X		
IDS_ANL.1			X		
IDS_RCT.1			X		
IDS_RDR.1	X	X			

The following table provides the detail of TOE security objective(s).

Table 18 - Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.ACCESS	This TOE Security Objective is satisfied by ensuring that: • FMT_MTD.1(1) and FMT_MTD.1(2): Only authorized user can perform the management functionality associated with their role as identified in these SFRs. • FMT_SMR.1: The TOE must be able to recognize the different roles that exist for the TOE. • IDS_RDR.1: The TOE must provide the ability for authorized administrators to view the data collected about databases.
O.EADMIN	This TOE Security Objective is satisfied by ensuring that: • FMT_SMF.1: The TOE must be capable of performing the security management functions. • IDS_RDR.1: The TOE must provide the ability for authorized administrators to view the data collected about databases.
O.IDACTS	This TOE Security Objective is satisfied by ensuring that: • IDS_SDC.1: The TOE is required to collect and store vulnerability and configuration information of a database. • IDS_ANL.1: The TOE is required to analyze the databases to detect vulnerabilities and suspicious behavior. • IDS_RCT.1: The TOE is required to generate alerts for configured conditions.
O.IDENT	This TOE Security Objective is satisfied by ensuring that: • FIA_ATD.1: Security attributes of subjects use to enforce the authentication policy of the TOE must be defined. • FIA_UID.2: The TOE requires each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.
O.PROTCT	This TOE Security Objective is satisfied by ensuring that: • FMT_MTD.1(1) and FMT_MTD.1(2): Only authorized user can perform the management functionality of the TOE identified in the table in FMT_MTD.1(1) and FMT_MTD.1(2).

9.2.2 Security Assurance Requirements Rationale

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

The general level of assurance for the TOE is:

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

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