National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

IBM

IBM Tivoli Security Operations Manager 4.1.1

Report Number: **CCEVS-VR-VID10092-2009**
Dated: **13 April 2009**
Version: **1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Mr. Jim Brosey
Orion Security
McLean, VA

Mr. Daniel P. Faigin
The Aerospace Corporation
El Segundo, California

Common Criteria Testing Laboratory

Ms. Cynthia Reese
Ms. Dawn Campbell

Science Applications International Corporation
Columbia, Maryland

Much of the material in this report was extracted from evaluation material prepared by the CCTL. The CCTL team deserves credit for their hard work in developing that material. Many of the product descriptions in this report were extracted from the IBM Tivoli Security Target.

Table of Contents

List of Figures

List of Tables

EXECUTIVE SUMMARY

This report documents the results of the Validation Panel's oversight of the evaluation of the IBM Corporation Tivoli Security Operations Manager (TSOM) product. It presents the evaluation results, justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) and was completed during March 2009. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by SAIC and submitted to the Validation Panel. The evaluation determined that the product conforms to the Common Criteria Version 2.3, Part 2 extended and Part 3 conformant and meets the requirements of Evaluation Assurance Level (EAL) 3.

The Target of Evaluation (TOE) is the IBM Tivoli Security Operations Manager, (hereafter referred to as the TOE or TSOM). The TOE is a security event management software solution designed to provide a comprehensive and coherent view of enterprise security. The TOE correlates event data from disparate machines outside the TOE, called sensors. Sensors are third-party products such as firewalls, intrusion detection systems, computer systems, and routers. Once data is correlated from sensors, the TOE analyzes the data to uncover legitimate threats to the enterprise.

The cryptography used in this product is provided by the IBM JSSE FIPS 140-2 Cryptographic Module, which was not analyzed within the scope of this evaluation. However, JSSE has received Federal Information Processing Standard (FIPS) 140-2 validation, as described in Certificate #409.

The Validation Team provided oversight on the activities of the evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the Common Evaluation Methodology (CEM) work units), and reviewed successive versions of the ETR and test report. The Validators' observations support the CCTL's conclusion that the product satisfies the functional and assurance requirements defined in the Security Target (ST). Therefore, the Validation Panel concludes that the findings of the evaluation team are accurate, and the conclusions justified.

1 IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List. **Table 1** provides information needed to completely identify the product.

Table 1 Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	IBM Tivoli Security Operations Manager 4.1.1
Protection Profile	None
Security Target	IBM Tivoli Security Operations Manager Security Target, version 1.0, 3/25/09
Evaluation Technical Report	Final Evaluation Technical Report for Tivoli Security Operations Manager , Part 1 Non-Proprietary, V1.3, March 30, 2009 Final Evaluation Technical Report for Tivoli Security Operations Manager , Part 1 Proprietary, v1.3, March 30, 2009 Final Evaluation Technical Report for Tivoli Security Operations Manager , Part 2 Proprietary, v1.3, March 30, 2009
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005. Part 2: Security functional requirements, Version 2.3, August 2005 Part 3: Security assurance requirements, Version 2.3, August 2005.
Conformance Result	Part 2 extended, Part 3 conformant, EAL3 conformant
Sponsor	IBM, Atlanta GA
Developer	IBM, Atlanta GA
Evaluators	SAIC, Columbia, MD
Validators	Mr. Daniel P. Faigin, The Aerospace Corporation Mr. Jim Brosey, Orion Security

2 SECURITY POLICY

The TOE supports the following security functions: Audit, Identification and Authentication, User Data Protection, Security Management, Protection of the TSF, IDS.

2.1 Audit Function

The TOE generates audit records that track the actions of authorized TOE users. The audit records are stored and protected in the underlying database in the IT environment of the TOE.[1] The IT environment also provides the timestamp for the audit records. Audit information may be accessed through the Event Console or the PowerGrid interface. Access to audit information is restricted to authorized administrators.

2.2 Identification and Authentication

User identification and authentication is required to access the user interface of the TOE. The user is always prompted for user name and password credentials before accessing the system. User account information is stored and protected by the database in the IT environment of the TOE. The TOE generates an MD5 hash of the user password. This hash is stored as part of the user account information in the IT environment. The user login process performs authentication as well as providing system privileges that are defined on a per-user or per-role basis. The User Interface is a Java-based rich client that is launched via a browser (such as Internet Explorer 6.0 or greater).

By default, the Account Lockout feature is disabled. In the evaluated configuration, this feature must be enabled by checking “Enable Account Lockout”. Once account lockout is enabled, the default number of authentication attempts and the default lockout time period will apply unless configured otherwise by the administrator.

2.3 User Data Protection

The TOE enforces an access control policy which defines the classes of objects that an authorized user of the TOE will have permission to manage and configure. These classes of objects includes security domains, rules that can be defined within the TOE, hosts, networks, events, tickets, and firewall rules.

2.4 Security Management

The TOE is designed to provide threat management for security incidents, which require handling many-to-one relationships. The Central Management System (CMS), in turn, correlates the data, determines the threat and presents the relevant information to the authorized user through either the Event Console or the PowerGrid interface. The TOE provides the user interface utilized by the authorized administrator to manage the security and network event data collection functions and attributes.

2.5 Protection of TSF

[1] The Errata [4] in the IDS Analyzer PP (referenced in Section 1.2) permits software TOEs to move the FAU_STG.2 requirement to the IT environment. In these cases, the PP also mandates that OE.AUDIT_PROTECTION be added to the ST which has been done. This environment objective requires that the environment protect the audit information.

The TOE ensures that TSF data is protected from disclosure and modification when it is transmitted between TOE components. The TOE invokes a FIPS validated module to encrypt communications between distributed parts of the TOE (UI, CMS, and EAM). The TOE also uses a separate SSL mechanism (i.e. not part of the FIPS module) to encrypt communications between the UCM and the EAM. Additionally, the TOE ensures that all TSF data is made available to distributed parts of the TOE.

The IT environment of the TOE provides various mechanisms to ensure that the access control policy is always enforced and the data transmitted between TOE components is protected. The IT environment, specifically the underlying Operating System (OS), supports the non-bypassability of the TSP by protecting itself and the TOE from external interference and tampering. The OS maintains a security domain for its own execution and enforces the separation between the security domains of subjects in the TSC.[2]

2.6 **IDS Function**

The TOE provides the functions for collecting, analyzing, review and response to the events that occur at the network sensors. Some of the responses available include interfacing with other elements of the IT Environment, such as sending SNMP Traps to a Trap receiver located in the IT Environment, or emails to an SMTP server located in the IT Environment.

The TOE has the ability to acquire GPS coordinates for hosts and networks seen in the events that flow through the CMS. This is accomplished through a connection from the CMS to an IBM-maintained server in the IT environment of the TOE.

[2] The Errata [3] in the IDS Analyzer PP (referenced in Section 1.2) permits software TOEs to move the FPT_RVM requirement to the IT environment. In any case, the FPT_RVM requirement is redundant with the FDP requirements regarding access control which are claimed in this ST and enforced by the TOE.

3 ASSUMPTIONS AND CLARIFICATION OF SCOPE

3.1 Assumptions Regarding Operation

3.1.1 Physical Assumptions

- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

3.1.2 Personnel Assumptions

- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
- The TOE can only be accessed by authorized users.

3.1.3 Intended Usage Assumptions

- The TOE has access to all the trusted IT System resources necessary to perform its functions and these resources are set up in such a manner that the TOE can perform its functions securely

3.2 Operating Environment

The IBM TSOM TOE is supported by trusted hardware and software in the IT environment that is set up and configured in a manner such that the TOE can perform its functions securely. The IT Environment of the TOE consists of the following:

- **A Linux/Unix or Windows operating system environment** (Redhat Enterprise Server, Solaris, AIX operating systems, or Windows Server 2003). The operating system supports the protection of TSF processes and data by providing TSF domain separation and non-bypassability. The TOE also relies on the operating system to provide a reliable time stamp for the audit and event records. The specific version of operating systems upon which the TOE can be installed are:
    - RedHat Linux ES 5.0
    - AIX 5L Version 5.31[3]
    - Sun Solaris 10 (SPARC)
    - Microsoft Windows 2003 R2 Enterprise Edition (64-bit)
- **A database** (DB2 or Oracle) for storing audit, event data and user account information. The

[3]It should be noted that when the CMS and the EAM are running on an IBM AIX server, neither firewall blocking nor the Check Point conduit are supported as Check Point does not currently provide OPSEC binaries for the IBM AIX platform.

database is an external interface into the IT Environment. All security functions required around the database are to be performed by the IT Administrators.

- **An internet browser** (Internet Explorer v.6 or later or Mozilla v1.3 or later), which is used to launch the Java-based User Interface
- **A Java Runtime Environment** (Java 5 JRE), which is used to support the Java-based User interface on the client machine.
- **Sensors**, which are disparate machines in the IT environment used by the TOE for data collection.
- **An SMTP Server and/or an SNMP Trap Receiver**, used by the TOE to send information and alerts via Email (SMTP) and SNMP Traps.
- **A connection to an IBM-maintained Geoserver**, which communicates with the geoclient embedded in the TSOM TOE application. This Geoserver is accessed via a connection from the CMS to geoloc.ibm.com using a proprietary XML based protocol.
- **Trusted DNS servers,** used by the TOE as part of the geoserver feature process as well as to resolve hostnames in email addresses.

Table 2 lists the security functional requirement that must be satisfied by the IT Environment as presented in the ST.

Table 2 IT Environment Security Functional Requirements

Security Functional Class	Security Functional Components
Security Audit (FAU)	FAU_STG.2: Guarantees of Audit Data Availability
Protection of the TSF (FPT)	FPT_RVM.1b Reference Mediation
	FPT_SEP.1 Domain Separation
	FPT_STM.1b Reliable Time Stamps

3.3 Clarification of Scope

The Security Target specifies the security requirements of the TOE, which determined the scope of the evaluation. The security requirements allocated to the IT environment have not been verified as part of the TSOM evaluation—it is the responsibility of the integrator to ensure the IT environment satisfies those requirements. The IT security services provided by the environment support the protection of the TOE Security Functions (TSF) including domain separation, reference mediation (preventing bypass of the security functions), and reliable time-stamps (used in time-stamping audit records).

The following features are *not* included in the evaluated configuration:

- **LDAP**, an alternate method of remote authentication. Enabling remote authentication will make any password policies set by the TOE unenforceable, since the password policy will be governed by the remote authentication server. By default, the remote authentication capability is disabled and will remain disabled in the evaluated configuration. This capability is not enabled in the TOE.

- **Host Investigative (HIT) Tools**, a toolkit that includes SNMP Get, TCP Port Scan, HTTP Probe, Traceroute, UDP Port Scan and TCPDUMP among others. The HIT toolkit is an optional component not included with the TOE.
- **Change Control Management database (CCMDB)**, an optional component that can be configured and then be used to store configuration information about hosts. The CCMDB is not within the scope of this evaluation and is not enabled in the TOE.
- **Vulnerability Import utility**, a command line utility used to import vulnerability data from a vulnerability scanner. Neither this utility nor vulnerability scanners in the IT environment are within the scope of this evaluation.
- **Compound threat calculation**, which is calculated using the average of atomic threats and the threat level generated by a host for two time periods. Compound threat calculation is not within the scope of this evaluation; while the TOE generates data from this type of analysis, this data was not subject to evaluation.

4 ARCHITECTURAL INFORMATION

The TOE is composed of the following subsystems:

- Event Aggregation Module (EAM)
- Universal Collection Module (UCM)
- Central Management System (CMS)

4.1 Event Aggregation Module

The Event Aggregation Module (EAM) gathers data from various third-party sensors, then normalizes, filters, batches and transmits that data to the Central Management System (CMS). The EAM provides the following functions:

- Interface to third-party Sensors
- Optional Filtering of Event Data
- Formatting Event Data into TSOM normalized format
- Secure transmission of the Event Data to the Central Management System

The EAM collects Security Event Data from third-party sensors such as Firewalls, Intrusion Detection Systems and Servers etc. For those devices that support standards based interfaces such as SNMP, SYSLOG and XML, TSOM uses device specific rules to interpret the data. For some devices, such as Checkpoint FW1, TSOM has developed an interface to their proprietary interfaces. Some devices do not support any appropriate mechanism to get the security event data from the device to the EAM; in these situations, TSOM deploys the UCM on the sensor that extracts the data locally on the device and then sends the data to the EAM over a secure interface.

The EAM can optionally filter out non-essential event data so that this data will not be sent to the CMS. Once the EAM has formatted event data, it transmits this data to CMS over a secure encrypted connection for correlation and permanent storage.

4.2 Universal Collection Module

The Universal Collection Module (UCM) is a platform agnostic data collection device. The UCM is used to gather data from security devices that reside on platforms that cannot support an EAM. The UCM can be deployed on any platform in the IT environment as long as the UCM has access to the data required. For example, the UCM might connect via JDBC to a database to query for updates. This situation is satisfactory as long as the platform the UCM has been deployed on has network access to both the database in question and the EAM. The UCM can also be configured to monitor a Windows event log or a directory used to store files containing event data. The UCM transfers the data gathered from the device to the EAM utilizing a proprietary XML format to communicate events to the EAM. This proprietary XML interface is solely used by the TOE to transport raw events from the UCM to the EAM.

4.3 Central Management System

The Central Management System (CMS) brings together event data streams from all of the EAMs deployed in a network. The CMS correlates the event data and a threat analysis is performed. The CMS caches a running subset of the correlated event data for real-time display, while directing the correlated

event data-stream to the archiver (ie. database) for persistent storage. Both the real-time and persistent data is used in presenting relevant information through the user interface and advanced analytics module.

4.3.1 Event Correlation and Threat Determination

Event correlation and threat determination involve a combination of embedded logic and configurable rules to correlate events while determining the threat level of each event.

The embedded logic performs many of the routine tasks currently performed by security analysts: sorting and determining the relationship between events, assigning a weighted threat value to each event, and associating each event to source and destination hosts.

The configurable rules provide a concurrent approach to threat determination. By applying stateless and stateful rules, the CMS screens the event stream against configurable enterprise-level attack signatures, and triggers actions based on these signatures.

4.3.2 Event Caching and Archiving

Once correlation and threat determination has been completed, the CMS caches a copy of the correlated event for real-time viewing. The event-stream is also directed to the Event archiver for persistent storage in the underlying audit and event database in the IT environment of the TOE. Event queries and reporting using analytical tools provided by the CMS are conducted from the events within this database.

The Correlation process performs the following actions upon data in the event cache:

- Dropping non essential events, user definable
- Atomic threat level calculations based upon the source and destination addresses of the event
- Business Rule processing of events (stateless and stateful analysis)
- Storage of the correlated events into the event ready cache

4.3.3 User Interface

The User Interface is a set of modules that access and update various in-memory and database tables for the presentation and maintenance of data within the system. Key components of the User Interface are:

- Event Console (Real Time Viewer)
- Power Grid
- Threat Displays
- Event Searching
- Host and Network queries
- Ticketing System
- System Administration

4.3.4 Supported Devices

The TOE comes pre-configured to accept security event data from numerous security devices. Devices using SYSLOG, SNMP, XML as well as enhanced support for Check Point, ISS, and Cisco devices are easily connected to the TOE without requiring software agents. This approach simplifies deployment and

eliminates the problems of updating and configuring remote agents while also eliminating the additional system load that agent-based technologies incur.

The two primary subsystems are the EAM and the CMS. There can only be one CMS, however, there can be many EAMs. The CMS and EAM's are distributed on separate machines. The User Interface is a rich Java-based client which is launched via a web browser such as IE 6.0 or higher. The Event Console (Real Time Viewer) runs as a Java application, which automatically downloads when activated if the Java Runtime Environment (JRE) is running on the desktop. The Power Grid interface provides a comprehensive view of audit and event data and allows the user to analyze and detect patterns in the data.

The major components of the TOE are identified in **Figure 1**.

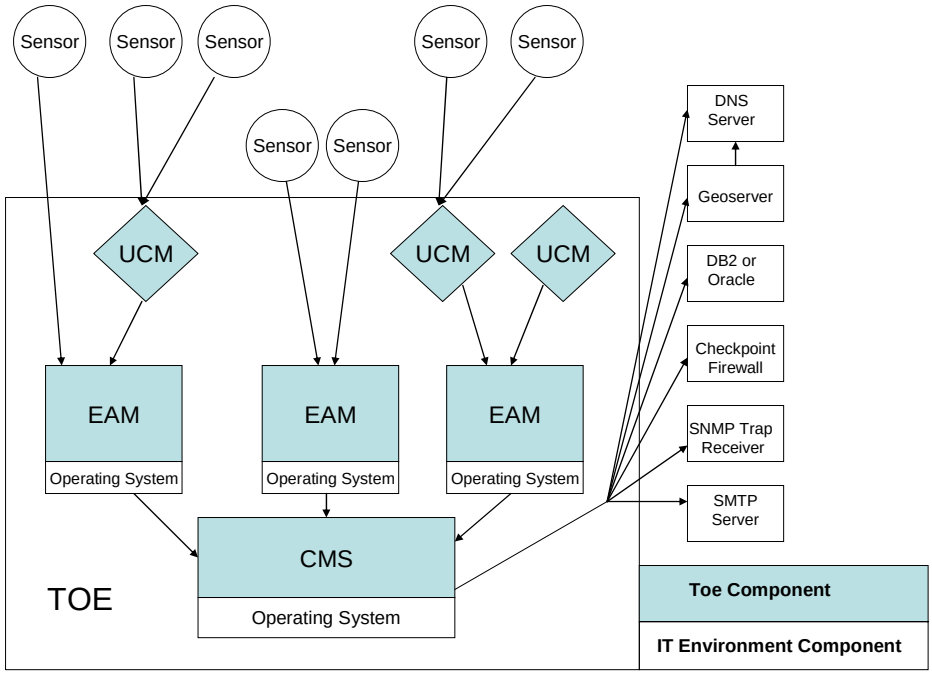

Figure 1. Tivoli Security Operations Manager System Architecture

5 DOCUMENTATION

The following documentation was used as evidence for the evaluation of the TOE. Of these, the Guidance documentation is available for download at the website:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.netcool_som.doc/welcome.htm

Documents with bolded names are publically available.

5.1 Design documentation

Document	Revision	Date
Tivoli Security Operations Manager Functional Specification	0.10	2009-03-05
Tivoli Security Operations Manager High Level Design	0.5	2009-03-05

5.2 Guidance documentation

Document	Revision	Date
Tivoli Security Operations Manager Version 4.1.1 Administration Guide	SC23-6100-01	2008-07
Tivoli Security Operations Manager Version 4.1.1 Installation Guide,	GC23-6099-01	2008-07
Tivoli Security Operations Manager Common Criteria Guide, Version 4.1.1	SC23-9743-01	2009-03-29
Tivoli Security Operations Manager Version 4.1 User Guide	SC23-6306-00	2008-01

5.3 Configuration Management and Lifecycle documentation

Document	Revision	Date
IBM Tivoli Security Operations Manager Configuration Management	0.5	2009-01-30
IBM Tivoli Security Operations Manager Life Cycle Support	0.3	2008-06-17

5.4 Delivery and Operation documentation

Document	Revision	Date
IBM Tivoli Security Operations Manager Delivery and Operation	0.5	2008-11-14

5.5 Test documentation

Document	Revision	Date
IBM Common Criteria Test Plan TSOM 4.1.1	1.7	2009-01-30

5.6 **Vulnerability Assessment documentation**

Document	Revision	Date
IBM Tivoli Security Operations Manager Vulnerability Assessment	0.5	2009-01-29

5.7 **Security Target**

Document	Revision	Date
IBM Tivoli Security Operations Manager Security Target	1.0	2009-03-25

6 IT PRODUCT TESTING

6.1 Vendor Testing

Testing of the TOE security functions was provided by a series of manual tests. These tests demonstrated the security-relevant behavior of the TOE at the interfaces identified in the Functional Specification document and defined in the High-Level Design documentation. The goal of these tests was to demonstrate that the TOE meets the security functional requirements specified in the Security Target.

At the same time that these tests demonstrated the behavior of the TOE interfaces, they also indirectly demonstrated the interfaces of the IT environment components upon which the TOE depends. These IT environment interfaces included the Geoserver and trusted DNS servers that the TOE relies on in order to implement its geoserver/geolocation functionality; the SMTP and SNMP servers used to implement some of its IDS functionality; and the CheckPoint Firewall for which the TOE provides enhanced support and firewall blocking.

The security functions tested were the same as those mentioned in the Security Target: Audit, Security Management, User Data Protection, Identification and Authentication, Protection of the TSF and Intrusion Detection. For the associated security functional requirements, please refer to the IBM Tivoli Security Operations Manager Security Target.

The evaluation team determined that the developer's actual test results matched the vendor's expected results.

6.2 Evaluation Team Independent Testing

The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the developer test documentation sufficiently addressed the TSFI and security functions as described in the functional specification. The evaluation team performed approximately 50% of the developer's test suite. The evaluation team devised and conducted an independent set of team tests and penetration tests. In some areas, the results of testing resulted in claims being removed from the Security Target.

7 EVALUATED CONFIGURATION

The TSOM v4.1.1 product is a software product that operates on the following operating system platforms:

- RedHat Linux ES 5.0
- AIX 5L Version 5.31[4]
- Sun Solaris 10 (SPARC)
- Microsoft Windows 2003 R2 Enterprise Edition (64-bit)

The operating environment includes the hardware platform, one of the above operating systems, the database platform (which can consist of DB2 or Oracle), the sensors, the browser (Internet Explorer v6 or later or Mozilla v1.3 or later) and the Java Runtime Environment (JRE) for access to installing the User Interface. The TOE is also dependent upon the use of a GeoServer and trusted DNS servers in the IT environment for its geoserver feature and upon SMTP and SNMP servers for aspects of its IDS functionality. The operating environment is not part of the TOE.

Each of the product components (UI, CMS, EAM) are run on different machines.

Note that TSOM v4.1.1 must be installed, configured, and operated according to the guidance documentation identified in Section 5.2, “Guidance documentation”.

[4]It should be noted that when the CMS and the EAM are running on an IBM AIX server, neither firewall blocking nor the Check Point conduit are supported as Check Point does not currently provide OPSEC binaries for the IBM AIX platform.

8 RESULTS OF THE EVALUATION

The evaluation was conducted based upon CC version 2.3 and CEM version 2.3. The evaluation determined the IBM TSOM v4.1.1 TOE to be Part 2 extended and Part 3 conformant, and that the TOE meets the Part 3 Evaluation Assurance Level (EAL3) requirements.

8.1 Evaluation of the Security Target (ST) (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

8.2 Evaluation of the CM capabilities (ACM)

The evaluation team applied each EAL3 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation. The evaluation team ensured the procedure included automated support to control and track changes to the implementation representation. The procedures reduce the risk that security flaws exist in the TOE implementation or TOE documentation.

8.3 Evaluation of the Delivery and Operation documents (ADO)

The evaluation team applied each EAL3 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification, the discrepancy between the developer master copy and the version received, and the detection of attempts to masquerade as the developer.

8.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL3 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification and a high-level design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

8.5 Evaluation of the guidance documents (AGD)

The evaluation team applied each EAL3 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE.

8.6 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL3 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities

during TOE development and maintenance. The evaluation team ensured the procedures described in the life-cycle model and tools are used to develop and maintain the TOE. The evaluation team also ensured the adequacy of the developer's flaw remediation procedures.

8.7 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL3 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE security functional requirements are enforced by the TOE. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team tests and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

8.8 Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL3 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, the evaluation team's misuse analysis and vulnerability analysis, and the evaluation team's performance of penetration tests.

8.9 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

8.10 Assurance Requirement Results

The assurance requirements for the TOE evaluation are those required by EAL3.

8.10.1 Common Criteria Assurance Components

The CEM work units associated with EAL3 are distributed amongst the ETR sections in Chapter 15 of the ETR. Collectively, the ETR sections in Chapter 15 encompass all CEM work units for EAL3. Each ETR section includes the CEM work units associated with that ETR section title (e.g. ACM). Within each ETR section, for each CEM work unit the following is provided:

- Verdict
- Verdict Rationale

The rationale justifies the verdict using the CC, the CEM, and any interpretations and the evaluation evidence examined. The rationale demonstrates how the evaluation evidence meets each aspect of the criteria.

The work performed contains a description of the action performed or the method used to apply the work unit.

8.10.2 Testing and Vulnerability Assessment

In addition to ETR sections, the evaluators developed a Test Plan/Report Part to capture the detail beyond the CEM work unit information. This detail is described within the CEM guidance for the testing and

vulnerability assessment work units. Primarily, the additional detail is focused on team test procedures, penetration test procedures, results from running the vendor's sample, and the justification of running the vendor's sample.

The evaluation team prepared a Draft of the Test Plan/Report prior to testing that addressed the selection of vendor tests to run, the team test procedures, and the penetration test procedures. After performing the test, the Test Report Part was updated to include the actual results from the vendor sample run and the team test. The Test Report is included in the "Final Evaluation Report Part II (Proprietary) For IBM Tivoli Security Operations Manager (TSOM)" ETR document, Chapter "Test Report".

8.11 **Conclusions**

The conclusions for the ST evaluations and the TOE evaluations are addressed below.

8.11.1 ST Evaluation

Each verdict for each CEM work unit in the ASE ETR is a "PASS". Therefore, the IBM Tivoli Security Operations Manager Security Target is a CC compliant ST.

8.11.2 TOE Evaluation

The verdicts for each CEM work unit in the ETR sections included in Chapter 15 are each "PASS". Therefore, the IBM TSOM TOE (see below product identification) satisfies the IBM Tivoli Security Operations Manager Security Target, when configured according to the guidance documentation identified in Section 5.2, "Guidance documentation."

8.12 **Summary of Evaluation Results**

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor test suite, the independent tests, and the penetration test further demonstrated the claims in the ST.

9 VALIDATOR COMMENTS AND RECOMMENDATIONS

The Validation Panel's observations support the evaluation team's conclusion that the TSOM v4.1.1 meets the claims stated in the Security Target. The following are some recommendations and guidance for those integrating this product into a system:

1) Authentication of sensors is not claimed in the Security Target, and therefore, was not covered by the evaluation. Note that authentication of sensors is also not required by the IDS Analyzer PP.

2) The product was tested to ensure the audit events and audit records contents were consistent with the claims in the Security Target. The Security Target was updated to remove specific claims based upon the testing results such as the ability to audit access to audit data and that the audit content includes the user identification of the user whose role is changed. Those integrating this product into a DOD or USG environment should verify that the set of events audited are appropriate for the audit controls that apply to the overall system (ECAR-*n* in DOD 8500.2, and the appropriate AU-*n* control and enhancements in NIST 800-53)

3) The product comes close to meeting the technical requirements of the DOD IAIA control, but cannot restrict the password to include lower case characters. It also does not appear to maintain a password history. When integrated into a DOD environment, compensating mechanisms may be required.

4) The TSOM product **must be** configured according to the TSOM Common Criteria Guide document to be in the evaluated configuration. This document specifies configuration settings such as enabling the account lockout feature and requiring password criteria such as a minimum of 8 characters.

10 SECURITY TARGET

The IBM document, IBM Tivoli Security Operations Manager Security Target, Version 1.0, 25 March 2009, is included here by reference.

11 GLOSSARY

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
CM	Configuration Management
DAC	Discretionary Access Control
DDL	Data Definition Language
DML	Data Manipulation Language
DRDA	Distributed Relational Database Architecture
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
LBAC	Label Based Access Control
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
PP	Protection Profile
RDBMS	Relational Database Management System
SFR	Security Functional Requirement
SQL	Structured Query Language
ST	Security Target
TCSEC	Trusted Computer System Evaluation Criteria
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface

12 BIBLIOGRAPHY

[1] COMMON CRITERIA PROJECT SPONSORING ORGANIZATIONS. *Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model,* August 2005, Version 2.3, CCMB-2005-08-001.

[2] COMMON CRITERIA PROJECT SPONSORING ORGANIZATIONS. *Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements,* August 2005, Version 2.3, CCMB-2005-08-002.

[3] COMMON CRITERIA PROJECT SPONSORING ORGANIZATIONS. *Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements,* August 2005, Version 2.3, CCMB-2005-08-003.

[4] COMMON CRITERIA PROJECT SPONSORING ORGANIZATIONS. *Common Evaluation Methodology for Information Technology Security: Evaluation Methodology*, August 2005, Version 2.3, CCMB-2005-08-004.

[5] COMMON CRITERIA PROJECT SPONSORING ORGANIZATIONS. *Part 2: Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation,* Version 1.1, February 2002, CEM-2001/0015R

[6] SCIENCE APPLICATIONS INTERNATIONAL CORPORATION, *Evaluation Technical Report for IBM TSOM Part 1 (Non-Proprietary)*, Revision 1.3, 30 March 2009.

[7] SCIENCE APPLICATIONS INTERNATIONAL CORPORATION, *Evaluation Technical Report for IBM TSOM Part 1 (Proprietary)*, Revision 1.3, 30 March 2009.

[8] SCIENCE APPLICATIONS INTERNATIONAL CORPORATION, *Evaluation Technical Report for IBM TSOM Part 2 (Proprietary)*, Revision 1.3, 30 March 2009.

[9] SCIENCE APPLICATIONS INTERNATIONAL CORPORATION *for* IBM. *IBM Corporation TSOM Security Target*, Version 1.0, 25 March 2009.

[10] COMMON CRITERIA EVALUATION AND VALIDATION SCHEME. *NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories,* Version 1.0, March 20, 2001, Scheme Publication #4.