National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Retina Enterprise Suite

Report Number:	**CCEVS-VR-07-0043**
Dated:	**25 May 2007**
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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Ralph Broom
Noblis
Jerome F Myers
The Aerospace Corporation

Common Criteria Testing Laboratory

Tony Apted
Eve Pierre
Quang Trinh
Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary

This document is intended to assist the end-user of this product with determining the suitability of the product in their environment. End-users should review both the Security Target (ST) which is where specific security claims are made, and this Validation Report (VR) which describes how those security claims were evaluated.

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Retina Enterprise Suite. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in May 2007. The evaluation was conducted in accordance with the requirements of the Common Criteria for Information Technology Security Evaluation, version 2.2. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is **Common Criteria Part 2 Extended** and **Common Criteria Part 3 Conformant**, and meets the assurance requirements of EAL 2.

Retina Enterprise Suite is an IDS-type product developed by eEye Digital Security Corporation. It is a non-disruptive network security scanner, meaning it is not invasive, nor does it interfere with the operation of the IT system being monitored. The TOE does not scan network traffic anomalies reported by sensors, as do some other types of IDS products. Rather the TOE scans hosts identified within a specific IP range. Ports on targeted hosts are monitored for specific activities and events identified in an audit policy. The TOE includes a management capability that provides an authorized administrator with the ability to manage multiple scanners in the enterprise network, collating the results of scans from the various scanners and highlighting potential vulnerabilities for remedial action.

The TOE is supported on Microsoft Windows NT 4.0 SP6a, 2000, 2003, and XP.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 2.2) for conformance to the Common Criteria for IT Security Evaluation (Version 2.2). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The technical information included in this report was obtained from the Evaluation Technical Report (ETR) Part 1 (non-proprietary) produced by SAIC, the Retina Enterprise Suite Security Target, and analysis performed by the Validation Team.

The validation team agrees that the CCTL presented appropriate rationales to support the Results of Evaluation presented in Section 5, and the Conclusions presented in Section 6 of the ETR. The validation team therefore concludes that the evaluation and the Pass results for the Retina Enterprise Suite is complete and correct.

2 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 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, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated
- The Security Target (ST), describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	Retina Enterprise Suite, comprising the following eEye components: • Retina Network Security Scanner Version 5.4.21.53 • REM Events Manager version 3.0.2.571 • REM Events Server version 2.2.0.194
ST:	Retina Enterprise Suite Security Target, Version 1.0, 25 May 2007
Evaluation Technical Report	Evaluation Technical Report for eEye Retina Enterprise Suite: • Part 1 (Non-Proprietary), Version 1.0, 31 May 2007 • Part 2 (Proprietary), Version 1.0, 31 May 2007

Item	Identifier
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.2
CEM Version	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 2.2, January 2004, CCIMB-2004-01-004
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	eEye Digital Security Corporation One Columbia Aliso Viejo, CA 92656
Developer	eEye Digital Security Corporation One Columbia Aliso Viejo, CA 92656
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD
CCEVS Validators	Ralph Broom, Noblis Jerome F Myers, The Aerospace Corporation

3 Security Policy

The Retina Enterprise Suite enforces the following security policies as described in the Security Target.

> ***Note:*** *Much of the description of the Retina Enterprise Suite security policy has been extracted and reworked from the Retina Enterprise Suite Security Target and Final ETR.*

3.1 Network Security System

The TOE scans hosts identified within a specific IP range against predefined audit policies (that are set at the granularity of a specific host or collection of hosts), to detect known potential vulnerabilities. The audit policies govern the collection of data regarding inappropriate activities on the IT systems the TOE monitors. The TOE collects the following information from targeted IT systems: security configuration changes; access control configuration; service configuration; authentication configuration; accountability policy configuration; and detected known vulnerabilities. The TOE also provides capabilities to review the data collected.

3.2 Security Management

The TOE (via the REM Events Manager application) provides web-based interfaces that can be used to access and manage TOE services. The TOE allows the built-in Administrator to create additional users and user groups, assign administration permissions to user groups, and assign users to user groups. In this way, the management of the TOE and of scanning of IT systems within the enterprise can be delegated and controlled based on IP addresses.

3.3 Identification and Authentication

All users attempting to access the management capabilities provided by the Events Manager must provide a valid userid and corresponding password. Access to the Retina Network Security Scanner component is controlled by the IT environment of the Scanner.

3.4 Protection of the TOE Security Functions (TSF)

The TOE ensures that the TOE Security Policy (TSP) enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

4 Assumptions

The following assumptions underlying the evaluation of Retina Network Security Scanner are identified in the Retina Network Security Scanner Security Target.

4.1 Usage Assumptions

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

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

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

4.2 Physical Assumptions

The processing resources of the TOE are assumed to be located within controlled access facilities that will prevent unauthorized physical access.

It is assumed that the TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

4.3 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 users 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.

4.4 System Assumptions

The TOE operating environment will provide protection to the TOE and its related data.

The TOE operating environment will provide reliable system time.

4.5 Clarification of Scope

The TOE relies on the underlying operating system and its security. The operating system on which the TOE is installed is outside the TOE and hence its security properties are not covered by this evaluation.

The following product features described in the guidance documentation for the TOE were not covered in the evaluation: use of the Audit Wizard; use of Retina Plug-ins; use of Auto-Update or the Enterprise Update Server (which will take the TOE out of its evaluated configuration); and use by the Retina Network Security Scanner component of a DSN to store collected Scanner data.

5 Architectural Information

Note: *The following architectural description is based on the description presented in Part 1 of the Retina Enterprise Suite ETR and in the Security Target.*

The TOE comprises the following subsystems:

- REM Events Manager
- REM Events Server
- Retina Network Security Scanner.

The Events Manager subsystem is a web server application that provides the administrative center for remotely monitoring, administering and reporting on Scanner audited events and creating scanner implemented auditing policies. Audit policies created at the Events Manager determine the events monitored by Retina Scanners for a specific range of IP addresses. Policies are sent from the Events Manager to the Events Server. The Events Manager provides access to audit policies based on user roles.

The Events Manager subsystem provides web-based interfaces that are made accessible using a web server and accessed by using a web browser. Web-based interfaces are provided to manage System data and generated events, as well as to define rules and audit policies. Interfaces to generate and review reports of System data and audit data are also provided. These reporting interfaces can assist administrators in planning, auditing, analyzing, and implementing network security scanner configurations.

The Events Server subsystem supports communication between the Retina Network Security Scanner and the Events Manager subsystems. The Events Server subsystem is a server application that provides the policy information created via the Events Manager to Scanners when a Scanner requests a policy update. All communication between the Events Server and Retina Network Security Scanner is secured using SSL.

The scanning engine contained within the Retina Network Security Scanner scans IP address ranges for specific information. One or more instances of the Scanner are supported in the evaluated configuration. The scan is a passive one and the scanning process is multithreaded, which allows the Retina Network Security Scanner to handle different targeted hosts at the same time. The services provided are mapped to specific types of vulnerabilities identified in the audit policy for the specific IP range.

The process of scanning a host occurs in roughly the following manner:

- ICMP ping: This step establishes if the host is responding.
- Target setup: The specific details of the target are built, such as MAC addresses, reverse DNS hostnames and other details.
- Syn Scan: Using a series of TCP syn packets, Retina Network Security Scanner scans the host to determine which ports are responding.
- Protocol Detection: Whenever a port is found to be open, after the TOE establishes a connection with the port, it determines the protocol of the service offered on the port using the port number and any protocol-specific information that is initially returned by the target when the connection is established.
- OS Detection: Using a series of packets designed to "fingerprint" the target operating system, Retina matches the output against a database of known operating systems.
- Audit Phase: The audit phase is effectively the second half of the scan and encompasses the basic "vulnerability" scan portion of the audit.

It is in the audit phase when the TOE applies the audit policy looking for specific services and protocols for the specific targeted host.

The Events Manager and Events Server subsystems are installed on the same host, which can be running Microsoft Windows NT 4.0 SP6a, 2000, 2003, or XP. The following components are also required in the IT environment to support Events Manager and Events Server:

- Microsoft SQL Server 2000
- Microsoft IIS
- Microsoft .Net Framework 1.1.

The Retina Network Security Scanner can be installed on machines running Microsoft Windows NT 4.0 SP6a, 2000, 2003, or XP.

Internet Explorer v6 is required to access the web-based Events Manager console. The IT environment is also relied upon to provide SSL to protect communications between the Retina Network Security Scanner and Events Server, and to secure web-based access to the Events Manager console.

6 Documentation

The following documentation is provided with the TOE and provides information pertinent to the installation, configuration, and operation of the TOE:

- REM Security Management Console Management Guide, v3.02, 2005
- REM Security Management Console Operations Guide, v3.02, 2005
- REM Security Management Console Administration Guide, v3.02, 2005
- REM Users Manual, REM-M-032803, 2003
- REM Manual Addendum, REM-EU-M-030305, v2.2.0, 2005
- Retina Network Security Scanner Users Manual, Revision 5-3-1, 2005
- Release Notes for REM Events Manager version 3.0.2
- Release Notes for REM Events Server version 2.2.0
- Release Notes for Retina Network Security Scanner version 5.4.21.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for the Retina Network Security Scanner, Version 0.2, 31 May 2007.

7.1 Developer Testing

At EAL2, testing must demonstrate correspondence between the tests and the functional specification. The developer testing provided coverage of all of the security functions identified in the ST. These security functions are:

- Identification and Authentication
- Network Security System
- Security Management
- Protection of the TSF.

The developer testing covered capabilities provided by the Events Manager GUI for managing users, user groups, and scans. The developer testing also relied on the results previously obtained for the Retina Network Security Scanner (evaluated as a separate TOE).

Developer testing was performed only on one of the supported platforms (Microsoft Windows Server 2003 SP1), since there are no code changes for other supported platforms. There is only a single set of installation and runtime TOE components. There are no differences in the services the TOE relies on from the IT Environment provided by the other supported platforms.

7.2 Evaluation Team Independent Testing

The evaluation team test configuration comprised the following computers:

- REM Events Manager and REM Events Server host:
    - Dell Dimension 370 with Intel Pentium 4 3.40 GHz CPU, 1GB RAM, 150 GB HDD
    - MS Windows Version 5.2 (Build 3790.srv03_sp1_rtm.050324-1447: Service Pack 1 (Windows Server 2003 Enterprise Edition)
    - Microsoft Virtual PC version 5.3.582.27, running:
        - MS Windows Version 5.2 (Build 3790.srv03_sp1_rtm.050324-1447: Service Pack 1 (Windows Server 2003 Enterprise Edition)
        - Internet Information Server (IIS) version 6.0
        - Microsoft SQL Server 2000 version 8.00.761
        - .Net Framework version 1.1
- Retina Network Security Scanner host:
    - Dell Latitude laptop with Mobile Intel Pentium 4-M 2.20 Ghz CPU, 512 MB RAM, 6 GB HDD
    - MS Windows Version 5.2 (Build 3790.srv03_sp1_rtm.050324-1447: Service Pack 1 (Windows Server 2003 Enterprise Edition)
    - Internet Explorer 6.0
- Windows target
    - Dell Dimension 370 with Intel Pentium 4 3.40 GHz CPU, 1GB RAM, 150 GB HDD
    - MS Windows Version 5.2 (Build 3790.srv03_sp1_rtm.050324-1447: Service Pack 1 (Windows Server 2003 Enterprise Edition))
- Unix target
    - Sun Microsystems SunBlade 150 with sparc processor, 512 MB RAM
    - Solaris 9 (SunOS Release 5.9 Generic_117171-14).

These computers were connected via a small LAN.

The evaluation team verified that the TOE was installed as is specified in the secure installation procedures, reran over 70% of the developer tests and verified the results on one platform, then developed and performed functional and vulnerability testing that augmented the developer testing by exercising different aspects of the security functionality.

The evaluation team performed the following additional functional tests:

- Identification/Authentication Failure: The developer's test suites focus on positive tests only. This test was intended to confirm that a user that failed to enter a correct userid and password did not gain access to TOE functionality. The test demonstrated that the TOE requires users to enter a correct userid and corresponding password in order to logon to the REM Events Manager.

- Minimum Password Length and User Account Options: The evaluation team identified in the management interface of the TOE capabilities for specifying various parameters associated with user accounts, including minimum password length and account lockout threshold, which are not described in the ST The test showed that the TOE enforces the configured minimum password length and the configured account lockout threshold.
- Password Alphabet: The developer's vulnerability analysis claims that passwords can use all 94 printable characters on a standard keyboard. The test showed that the TOE accepts passwords comprising any of the 94 printable characters of a standard keyboard.
- Security Management Roles: The developer's test suites focus on positive tests only. This test was intended to confirm that user's assigned to roles are restricted to the capabilities specified for those roles. The test showed the TOE enforces management restrictions so that users have access only to the capabilities granted to the group they belong to.

The evaluation team performed the following vulnerability tests:

- Credential grabbing during a vulnerability scan: The TOE allows authorized users to enter username and password (I&A credentials) of machines to be scanned. The evaluation team attempted to ascertain the password using a network sniffer. The evaluation team determined credentials used in a scan are protected when sent over the network by the TOE.
- TOE Installation Protection: The TOE relies on the underlying operating system to protect it from tampering and bypass, and to protect the stored scanner data and other configuration data. The evaluation team, operating as an unprivileged user on the server hosting the Events Manager and Events Server, attempted to interfere with the operation of the TOE and its data. The evaluation team determined the underlying operating system provides adequate protection to the TOE and its data from unauthorized users.
- TOE Console Vulnerability: The TOE console is a web-enabled service that appears to allow browsers to connect using http. It is therefore possible that the user's password may be vulnerable to a network sniffer if the user attempts to access the TOE console from a remote computer (rather than from the Events Manager host computer). As expected, the administrator password was readily captured by the packet sniffer when the client attempted to login to the Events Manager. However, the TOE is able to and can be configured to require SSL communication from clients attempting to access the Events Manager console. The evaluation team followed the procedures described in Section 5 of the REM Security Management Console Administration Guide to configure Events Manager to require SSL connections. The evaluation team confirmed that once configured, it was not

possible to access the Events Manager console over an unsecured link. The user had to connect using https.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Retina Enterprise Suite, comprising the following eEye components:

- REM version 3.0.2.571
- REM Events Server version 2.2.0.194
- Retina Network Security Scanner Version 5.4.21.53

All components are supported on the following Microsoft Windows platforms: NT 4.0 SP6a, 2000, 2003, and XP.

To use the product in the evaluated configuration, the product must be installed and configured as specified in the following documentation:

- REM Security Management Console Administration Guide, v3.02, 2005
- REM Users Manual, REM-M-032803, 2003
- REM Manual Addendum, REM-EU-M-030305, v2.2.0, 2005
- Retina Network Security Scanner Users Manual, Revision 5-3-1, 2005
- Release Notes for REM Events Manager version 3.0.2
- Release Notes for REM Events Server version 2.2.0
- Release Notes for Retina Network Security Scanner version 5.4.21.

9 Results of the Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 2.2 and CEM version 2.2 [1]–[5]. The evaluation determined the Retina Enterprise Suite TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 2) requirements. The rationale supporting each CEM work unit verdict is recorded in the **Evaluation Technical Report for eEye Retina Enterprise Suite Part 2** which is considered proprietary.

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 the vendor tests suite, the independent tests, and the penetration tests also demonstrated the accuracy of the claims in the ST.

Under the Validation Oversight Review (VOR) process, the Validators review EAL2 evaluation evidence twice; at the Initial VOR and the Final VOR. The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

Validator comments and recommendations have been captured in Section 4.5 Clarifications of Scope and other sections.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as *Retina Enterprise Suite Security Target, Version 1.0, 25 May 2007*.

13 Glossary

The following definitions are used throughout this document:

- **Authentication.** Verification of the identity of a user or the user's eligibility to access an object.
- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.

- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 2.2, January 2004.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 2.2, January 2004.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 2.2, January 2004.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 1: Introduction and general model, Version 0.6, 11 January 1997.

[5] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 2.2, January 2004.

[6] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[7] Science Applications International Corporation. *Evaluation Technical Report for eEye Retina Enterprise Part 1*, Version 1.0, 31 May 2007.

[8] Science Applications International Corporation. *Evaluation Technical Report for eEye Retina Enterprise Suite Part 2 (SAIC and eEye Proprietary),* Version 1.0, 31 May 2007.

[9] Science Applications International Corporation. *Evaluation Team Test Report for eEye Retina Enterprise Suite, ETR Part 2 Supplement (SAIC and eEye Proprietary),* Version 1.0, 31 May 2007.

Note: This document was used only to develop summary information regarding the testing performed by the CCTL.

[10] Science Applications International Corporation. *Retina Enterprise Suite Security Target, Version 1.0, 25 May 2007*