National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

SolarWinds® ORION® Software

Report Number: **CCEVS-VR-VID10453-2012**

Dated: **June 18, 2012**

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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Mr. Paul A. Bicknell

The MITRE Corporation
Bedford, MA

Ms. Jean Hung

The MITRE Corporation
McLean, Virginia

Common Criteria Testing Laboratory

Mr. Herb Markle

CygnaCom Solutions
McLean, Virginia

Table of Contents

1. Executive Summary

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

This report documents the assessment by the National Information Assurance Partnership (NIAP) validation team of the evaluation of the *SolarWinds® ORION® Software*, the target of evaluation (TOE), performed by CygnaCom Solutions. It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by CygnaCom Solutions of McLean, VA in accordance with the United States evaluation scheme and completed on 30 April 2012. The information in this report is largely derived from the ST, the Evaluation Technical Report (ETR) and the functional testing report. The ST was written by Common Criteria Consulting LLC on behalf of SolarWinds. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, dated July 2009 at Evaluation Assurance Level 2 (EAL 2), and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1, Revision 3, dated July 2009.

Orion is a set of applications executing on one or more Windows servers. The applications monitor a configured set of network devices and applications for status, performance and configuration settings. Depending on the size of the network, multiple instances of the applications may be deployed on different servers to provide adequate performance.

This Validation Report (VR) documents the evaluation and validation of the product *SolarWinds® ORION® Software*.

This VR is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The Target of Evaluation (TOE) is a Network Management software suite that consists of the following components:

- SolarWinds Orion Network Performance Monitor (NPM) V10.1.3,
- Orion Application Performance Monitor (APM) V4.0.0,
- Orion Network Configuration Manager (NCM) V6.1.0,
- Orion Netflow Traffic Analyzer (NTA) V3.7.0,
- Orion IP Address Manager (IPAM) V1.7.0,
- Orion IP SLA Manager (IPSLA) V3.5.0, and
- Orion Enterprise Operations Console (EOC) V1.3.0

2. Identification

Target of Evaluation: *SolarWinds ORION® Software*

Evaluated Software and Hardware:

SolarWinds® ORION® Software:

- SolarWinds Orion Network Performance Monitor (NPM) V10.1.3,
- Orion Application Performance Monitor (APM) V4.0.0,
- Orion Network Configuration Manager (NCM) V6.1.0,
- Orion Netflow Traffic Analyzer (NTA) V3.7.0,
- Orion IP Address Manager (IPAM) V1.7.0,
- Orion IP SLA Manager (IPSLA) V3.5.0, and
- Orion Enterprise Operations Console (EOC) V1.3.0

Developer:	SolarWinds Worldwide, LLC
CCTL:	CygnaCom Solutions 7925 Jones Branch Dr, Suite 5400 McLean, VA 22102-3321
Evaluators:	Herb Markle
Validation Scheme:	National Information Assurance Partnership CCEVS
Validators:	Paul A. Bicknell, Jean Hung
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 3.1 R3, July 2009
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 3.1 R3, July 2009

3. Security Policy

The TOE enforces the following security policies as described in the ST:

3.1.Identification and Authentication

When a connection is established to any of the Web Consoles, the TOE prompts the user for login credentials. The credentials are validated by the TOE for the Orion Server Web Console. For the EOC and NCM Web Consoles, the credentials are first passed to Windows for validation. For Windows application providing configuration capabilities for NCM, the TOE prompts the user for login credentials. If the credentials are valid, the username is used to retrieve the user's security attributes inside the TOE from the TOE database.

3.2.Management

Management functionality is provided to authorized users. The functionality provided to individual users is determined by the user's role, which is one of the security attributes for users.

3.3.Network Monitoring

The status and performance of managed elements are monitored. The results are saved and may be viewed by authorized users. Access to data about the managed elements may be limited by view limitations. Alerts may be generated in respond to configured conditions detected about the managed elements.

3.4.Configuration Management

The configurations of network devices may be downloaded from the network device, saved in the TOE database, and compared to a reference configuration. If a configuration change is detected, an upload of a saved configuration for the network device may be triggered.

3.5.Assumptions

The ST identifies the following assumptions about the use of the product:

1. The TOE has access to all the IT System data it needs to perform its functions.
2. The TOE is appropriately scalable to the IT Systems the TOE monitors.
3. Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users.
4. The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.

5. The Administrator will install and configure the TOE according to the administrator guidance.
6. There will be a network that supports communication between distributed components of the TOE. This network functions properly.
7. Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and on-going.

3.6.Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 2 in this case).
2. This evaluation only covers the specific version of the product identified in this document, and not any earlier or later versions released or in process.
3. As with all EAL 2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
4. Cryptographic protection is provided by the TOE; however, the cryptography used in this product was not analyzed or tested to conform to cryptographic standards during this evaluation.
5. The following product components and functionality will not be included in the TOE or the evaluation:
    a. Create a custom poller to monitor any SNMP-enabled device, collect detailed data from MIB tables, & monitor virtually any statistic available on network devices.
    b. Install additional polling engines for large networks with a small number of NPM or APM instances.
    c. Install additional web servers to support a large number of network managers.
    d. External web sites are not added to Orion Server Web Console views.
    e. The “Check for product updates” function is not used.
    f. Custom device pollers are not configured. Pollers supplied with the TOE are included in the evaluation.
    g. Custom component monitors are not configured. Component monitors supplied with the TOE are included in the evaluation. Account limitations are tied to custom component monitors and are also not configured.

h. Custom property functionality is not configured. Built-in properties are included in the evaluation.

i. Advanced Alerts (which use custom properties) are not configured. Basic Alerts are included in the evaluation.

j. Orion Server failover functionality is not configured.

k. The functionality to remotely manage interfaces in Network Devices.

l. Custom NCM device templates are not configured. The default device templates supplied with the TOE are included in the evaluation.

m. Customized views are not configured on Orion Server Web Consoles; default Views are used (the Allow Account to Customize Views permission may be set to allow specification of credentials for the NCM Integration Module).

n. View Limitations are not configured.

o. Customized page views are not configured on EOC Server Web Consoles; default page views are used (the Allow User To Personalize Their Pages permission is not set).

6. The Operational Environment needs to provide the following capabilities:

EOC Server Minimum Hardware and Software Requirements

Item	Requirements
Operating System	32-bit or 64-bit Microsoft Windows Server 2003 or Windows Server 2008 (including R2)
Web Server	Internet Information Service 6.0 or later
.NET Framework	Version 3.5 or later
CPU	3.0 GHz
Memory	2 GB
Available Disk Space	100 MB
DBMS	Microsoft SQL Server 2005 or SQL Server 2008. Express, Standard, or Enterprise

Orion Server Minimum Software Requirements

Item	Requirements
Operating System	Windows Server 2003 or 2008, including R2
Web Server	Microsoft IIS, version 6.0 and higher, in 32-bit mode
.NET Framework	Version 3.5 SP1 or later ASP .NET 2.0 Ajax Extension, Version 1 or later
SNMP Trap Services	Windows operating system management and monitoring tools
Web Browser	Microsoft Internet Explorer version 6 or higher with Active scripting, or Firefox 3.0 or higher

The hardware requirements for Orion Servers are dependent on the number of elements to be monitored and/or managed by the server.

Orion Server Minimum Hardware Requirements

Item	Requirements		
	<500 Elements	<2000 Elements	2000+ Elements
CPU	2.0 GHz	2.4 GHz	3.0 GHz
Memory	3 GB	4 GB	4 GB
Available Disk Space	2 GB	5 GB	20 GB

In addition to these platforms, the database used by the TOE is installed on a dedicated server with the DBMS. Each Orion Server requires its own Database Server.

Database Server Minimum Software Requirements

Item	Requirements
DBMS	SQL Server 2005 SP1 Express, Standard, or Enterprise; or SQL Server 2008 Standard, or Enterprise
Operating System	Any Windows OS satisfying the minimum requirements for the DBMS
Additional Software	SQL Server System Common Language Runtime (CLR) Types Microsoft SQL Server Native Client Microsoft SQL Server Management Objects

The hardware requirements for Database Servers are dependent on the number of elements to be monitored and/or managed by the associated Orion Server.

Database Server Minimum Hardware Requirements

Item	Requirements		
	<500 Elements	<2000 Elements	2000+ Elements
CPU	2.0 GHz	2.4 GHz	3.0 GHz
Memory	2 GB	3 GB	4 GB
Available Disk Space	2 GB	5 GB	20 GB

Credential validation for the EOC Web Console and NCM Web Console interfaces is performed by Windows locally or via Active Directory. The credentials supplied by the user to the TOE are passed to Windows for validation. If credential validation is successful, the same username is used to associate attributes with the user session in the TOE. Credential validation for the Orion Server Web Console is performed entirely by the TOE.

The evaluated configuration requires that IIS is configured to require secure (HTTPS) connections on all the servers hosting TOE components. This requirement protects any credentials supplied by remote users from disclosure.

When connecting to network devices, the TOE supports the use of SSH as well as Telnet. Files transferred from the network devices to the TOE may use SFTP or SCP. The SSL functionality used for these operations is provided by the operational environment.

4. Architectural Information

Orion is a set of applications executing on one or more Windows servers. The applications monitor a configured set of network devices and applications for status, performance and configuration settings. Depending on the size of the network, multiple instances of the applications may be deployed on different servers to provide adequate performance.

The Orion family consists of the following network, application, system, and storage monitoring and management products:

Orion Network Performance Monitor - Orion Network Performance Monitor (Orion NPM) provides the ability to detect, diagnose, and resolve performance issues with a dynamic network. It delivers real-time views and dashboards to visually display network performance. Automated network discovery features enable network managers to keep up with evolving networks.

Orion Application Performance Monitor - Orion Application Performance Monitor (Orion APM) brings monitoring, alerting, and reporting capabilities to applications and servers. Automatically discovers applications and provides visibility into application performance and the underlying operating systems and servers they run on.

Orion Network Configuration Manager - Orion Network Configuration Manager (Orion NCM) notifies network managers in real-time when device configurations change, helping network managers determine which changes could potentially cause network issues. Orion NCM also provides nightly configuration backups, bulk configuration changes, user tracking, and inventory and compliance reporting.

Orion NetFlow Traffic Analyzer - Orion NetFlow Traffic Analyzer (Orion NTA) enables network managers to quantify exactly how a network is being used, by whom, and for what purpose. The application mapping feature correlates the traffic arriving from designated ports, source IPs, destination IPs, and protocols to application names network managers can recognize. Orion NTA provides a comprehensive view of the network traffic, enabling network managers to find the bottlenecks or identify the bandwidth hogs.

Orion IP Address Manager - Orion IP Address Manager (Orion IPAM) is an IP address management module that enables network managers to create, schedule, and share IP address space reports. With either Orion NPM or Orion APM, Orion IPAM provides IP address management that is unified with performance monitoring data for a comprehensive view of network health.

Orion IP SLA Manager - Orion IP SLA Manager delivers a network monitoring solution for identifying site-specific and WAN-related performance issues from the perspective of each of the remote sites. With this Orion module, network managers can utilize Cisco IP SLA technology with automatic IP SLA setup to monitor key WAN performance metrics, including Cisco VoIP jitter and MOS.

Orion Enterprise Operations Console - Orion Enterprise Operations Console (Orion EOC) provides a consolidated command center to remotely monitor critical network infrastructure in multiple different physical locations. Orion EOC provides a consolidated command center to monitor the entire enterprise network and gives network managers unified visibility into remote Orion servers running either Orion NPM or Orion APM and Orion modules.

5. Documentation

The TOE is physically delivered to the End-User. The guidance is part of the TOE and is delivered as PDFs on the installation media.

5.1.Guidance Documentation

The following documents are developed and maintained by SolarWinds and delivered to the end user of the TOE:

Document Name	Version	Source
SolarWinds® Orion® Common Components Administrator Guide	V2010.2, 12.08.2010	SolarWinds
SolarWinds® Orion® Network Performance Monitor Administrator Guide	V10.1.3, 5.31.2011	SolarWinds
SolarWinds® Orion® Application Performance Monitor Administrator Guide	V4.0, 10.14.2010	SolarWinds
SolarWinds® Orion® Enterprise Operations Console Administrator Guide	v1.3, 2.11.2011	SolarWinds
SolarWinds® Orion® IP SLA Manager Administrator Guide	V3.5, 7.1.2010	SolarWinds
SolarWinds® Orion® NetFlow Traffic Analyzer Administrator Guide	V 3.7, 08.10.2010	SolarWinds
SolarWinds® Orion® IP Address Manager Administrator Guide	V1.7, 8-17-10	SolarWinds
SolarWinds® Orion® Network Configuration Manager Administrator Guide	V6.1, 04.01.2010	SolarWinds
SolarWinds® Orion® Common Criteria Supplement	V1.2, 02.24.2012	SolarWinds

5.2.Security Target (ST)

Security Target (ST)

[1] *SolarWinds ORION® Software Security Target*, Version 1.8, March 23, 2012

6. IT Product Testing

At EAL 2, the overall purpose of the testing activity is to “demonstrate that the TOE operates in accordance with its design representations and guidance documents” and independently confirm security functionality claims made in the ST.

The developer’s test evidence must “show the correspondence between the tests in the test documentation and the TSFIs in the functional specification” and demonstrate “the extent to which they are sufficient to demonstrate that the TSFI (see Functional specification (ADV_FSP)) perform as specified.”

The objective of the Evaluator’s independent testing sub-activity “is to demonstrate that the TOE operates in accordance with its design representations and guidance documents.” As part of this sub-activity the “evaluator also executes a subset of the developer's tests as documented to gain confidence in the developer's test results”. This section describes the testing efforts of both the Vendor and the evaluation team.

6.1.Developer Testing

The developer testing effort involved executing all the TOE’s described functions.

6.1.1. Overall Test Approach

All of the Developer test cases are manual, i.e. all test steps including setup and cleanup steps were performed by a user entering commands via the various web console interfaces and visually verifying the results. All developer test cases test TOE security functions by stimulating an external interface.

Although the developer tests are performed using the web consoles, the Evaluator determined that the test cases as described in the test documentation adequately exercise the internal interfaces.

The Developer executed all of their test procedures and provided a report of the actual results (screenshots included within the tests procedures). The Developer's actual results (screenshots) were consistent with their expected results (screenshots within test procedures) for the test procedures provided. All actual results were visually compared and verified before test was considered successful.

6.1.2. Test Results

The Developer's tests covered all of the security relevant behavior of the TOE:

- 85% of the External TSF Interfaces were tested.
- 80% of each subsystem’s described security features and behaviour

The Developer ran the test suite twice. Once in Jan and then again after it was determined NPM needed to be upgraded to 10.1.3.

- 100% of the tests were run successfully in both cases.

6.2.Evaluator Independent Testing

The testing was performed from the Evaluator's Home Office in Canastota, NY.

The Evaluator performed the following activities during independent testing:

- Installation of TOE
- Execution the Developer's Functional Tests
- Team-Defined Functional Testing
- Vulnerability/Penetration Testing

6.2.1. Execution of Installation Procedures

The execution of installation procedures was successfully accomplished. No additional steps were required to be added to either the administrative manuals of the CC supplement.

Identification of the TOE components based on the ACL description was successful. One small discrepancy (typo) was discovered and reported to SolarWinds and was entered into their bug tracking system. It was agreed upon that it was not necessary to change for the evaluation.

6.2.2. Execution the Developer's Functional Tests

The sampling of the Developer's Functional test cases was executed after the TOE was installed in the evaluated configuration consistent with the Security Target.

The Evaluator chose to execute ALL the Developer Functional tests to provide:

- verification of same environment, and
- new application build that was released after evaluation of ACM and IGS were completed
- gain confidence in functions
- ensure all human interfaces were stimulate
- stimulate optional external interfaces such as the SMTP server

.

The test configurations used by the Evaluator was equivalent as that used by the developer.

The test results and screenshots for the test cases were recorded during the Evaluator testing. Overall success of the testing was measured by 100% of the retests being consistent with expected results. No Anomalies were found during this stage of testing.

All of the Developer's Functional Tests rerun by the Evaluator received a 'Pass' verdict.

6.2.3. Evaluator-Defined Functional Testing

The evaluation team's strategy in developing the team-defined tests of the TOE was to supplement the developer functional tests and the penetration tests. The developer functional tests written by the vendor provided complete coverage of the security functional interfaces but not SFRs for the TOE as described in the ST. Therefore, the team tests are designed to ensure SFR descriptions were correct.

IND testing consisted of using the Developer's tests as the basis of running all of the IND tests. Deviations from their tests were used in order to ensure SFR coverage. In most cases the deviations are extremely obvious and were shown by a screenshots (such as showing all the attributes was done by clicking on the selection and showing the options and taking a screenshot. Deviations that required more information was documented in the Test Report.

All team tests were executed without issue. The evaluator is satisfied that the product operates as claimed in the ST and FSP. External Interface testing coverage was 100%. SFR coverage of testing was around 95% as it is impossible to hit every combination for every management function and combination (such as produce every event to test all event alerts).

6.2.4. Vulnerability/Penetration Testing

The Penetration tests for TOE were developed according to the following strategy:

- The Evaluator will perform a systematic vulnerability analysis of the TOE.
- The Evaluator will note possible security vulnerabilities by examining the Vulnerability Analysis, Functional Specification, TOE Design Document and TOE Security Target.
- The Evaluator will analyze the different components that comprise the TOE for existing vulnerabilities.
- The Evaluator will search public vulnerability databases for vulnerabilities that corresponded to these components.
- The Evaluator will identify hypothesized vulnerabilities requiring low attack potential that apply to the TOE.
- The Penetration tests will cover hypothesized vulnerabilities and potential misuse of guidance.
- The tests for potential misuse of guidance will cover installing the TOE from the guidance documentation and sampling the documented administrator procedures.

The Evaluator examined the external interfaces for means to bypass security. Scenarios for penetration testing were developed during vulnerability analysis of the product and after the Evaluator gained familiarity with the operation of the TOE.

- Testing included verification of cross-site scripting vulnerability was successfully mitigated (re-running Developer's Test 9)

- Buffer overflow testing on login screens and other free text input areas.

- Use of invalid characters when entering parameters
- OS/DB/TOE users are separate and cannot access the wrong environment accidentally (i.e., TOE user can’t login to the DB successfully)
- Port scan that showed 3 ports (none of which was needed for the TOE to operate correctly, all 3 were needed for evaluator to remotely test) This test showed the host OS was properly locked down.

All of the Vulnerability/Penetration Tests received a ‘Pass’ verdict.

7. Evaluated Configuration

The evaluated configuration consists of the following:

- One instance of the EOC, installed on a dedicated Windows server.
- One or more instances of the Orion Server, each installed on a dedicated Windows server. Each Orion Server has one or both of NPM and APM installed. Each Orion Server may have any combination of NCM, NTA, IPAM and/or IPSLA installed. If NCM is installed, the Orion Server integration module is also installed.
- For each instance of the Orion Server, a database (and DBMS) is installed on a separate dedicated Windows server.
- Installation and configuration options that must be used are included in administrative guidance entitled *SolarWinds Orion CC Supplement v1.2.*

Testing was performed on the Evaluated Configuration of the product using the Operational Environment and the Assumptions regarding the security environment as defined in the Security Target.

8. Results of Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1R3. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1R3.

CygnaCom Solutions has determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 2. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation effort was finished on April 30, 2012. A final Validation Oversight Review (VOR) was held on May 24, 2012 and final changes to the VR were completed on June 12, 2012.

9. Validators Comments/Recommendations

Vulnerability analysis of the TOE revealed a potential problem within the TOE. However, there are no known exploits, the degree of expertise required for an exploit is beyond what is expected to be protected against at EAL 2, and the vulnerability is in a portion of the TOE that was technically out of scope. For those reasons, Validators concluded that it was not necessary to resolve this potential problem in the TOE.

In addition, a version number mismatch found during IND testing. The CM and Guidance documentation only discuss finding the version number by using the TOE's web UI. However, it was discovered that Window's Program Uninstaller incorrectly reported the version number as a 4 digit number (A.B.C.D) where the 3rd and 4th set of numbers were reversed (A.B.D.C), but major and minor number (which is the TOE identifier) are correct and the installer file was correctly labeled. The bug was reported and is now being tracked by the Vendor. The Validators consider this a minor issue and are satisfied that the evaluated version of the TOE can be successfully determined.

10. Security Target

SolarWinds ORION® Software Security Target, Version 1.8, March 23, 2012, is compliant with the Specification of Security Targets requirements found within Annex B of Part 1of the CC.

11. Glossary

11.1. Acronyms

The following are product specific and CC specific acronyms. Not all of these acronyms are used in this document.

APM	**ORION Application Performance Monitor™**
CC	**Common Criteria**
CIDR	**Classless Internet Domain Routing**
DBMS	**DataBase Management System**
DHCP	**Dynamic Host Configuration Protocol**
DNS	**Domain Name System**
EAL	**Evaluation Assurance Level**
EOC	**Enterprise Operations Console**
FTP	**File Transfer Protocol**
HTTP	**HyperText Transfer Protocol**
HTTPS	**HTTP Secure**
ICMP	**Internet Control Message Protocol**
IMAP	**Internet Message Access Protocol**
IP	**Internet Protocol**
IPAM	**ORION IP Address Manager™**
IPSLA	**ORION IP SLA Manager™**
IT	**Information Technology**
MOS	**Mean Opinion Score**
NCM	**ORION Network Configuration Manager™**
NPM	**ORION Network Performance Monitor™**
NTA	**ORION NetFlow Traffic Analyzer™**
POP	**Post Office Protocol**
SCP	**Secure CoPy**
SFTP	**Secure FTP**
SLA	**Service Level Agreement**
SNMP	**Simple Network Management Protocol**
SSH	**Secure SHell**
SSL	**Secure Socket Layer**
ST	**Security Target**

TCP	**Transmission Control Protocol**
TOE	**Target of Evaluation**
ToS	**Type of Service**
TSF	**TOE Security Function**
UDP	**User Datagram Protocol**
URL	**Uniform Resource Locator**
VoIP	**Voice over IP**
WAN	**Wide Area Network**
WMI	**Windows Management Instrumentation**

12. Bibliography

URLs

[1] Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap-ccevs.org/cc-scheme).

[2] CygnaCom Solutions CCTL (http://www.cygnacom.com).

CCEVS Documents

[1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, July 2009 Version 3.1 Revision 3 Final, CCMB-2009-07-001.

[2] Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, July 2009 Version 3.1 Revision 3 Final, CCMB-2009-07-002.

[3] Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, July 2009, Version 3.1 Revision 3 Final, CCMB-2009-07-003.

[4] Common Methodology for Information Technology Security Evaluation - Evaluation methodology, July 2009, Version 3.1 Revision 3 Final, CCMB-2009-07-004.