Certificate Report

Version 1.0

2 August 2022

CSA_CC_20001

For

SolarWinds Security Event Manager v2019.4

From

SolarWinds Worldwide, LLC

This page is left blank intentionally

Foreword

Singapore is a Common Criteria Certificate Authorising Nation under the Common Criteria Recognition Arrangement (CCRA). The current list of signatory nations and approved certification schemes can be found at the CCRA portal:

https://www.commoncriteriaportal.org

The Singapore Common Criteria Scheme (SCCS) is established for the info-communications technology (ICT) industry to evaluate and certify their IT products against the requirements of the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 (ISO/IEC 15408) and Common Methodology for Information Technology Security Evaluation (CEM) Version 3.1 (ISO/IEC 18045) in Singapore.

The SCCS is owned and managed by the Certification Body (CB) under the ambit of Cyber Security Agency of Singapore (CSA).

The SCCS certification signifies that the target of evaluation (TOE) under evaluation has been assessed and found to provide the specified IT security assurance. However, certification does not guarantee absolute security and should always be read with the particular set of threats sought to be addressed and assumptions made in the process of evaluation.

This certification is not an endorsement of the product.

Amendment Record

Version	Date	Changes
1.0	2 August 2022	Released

NOTICE

The Cyber Security Agency of Singapore makes no warranty of any kind with regard to this material and shall not be liable for errors contained herein or for incidental or consequential damages in connection with the use of this material.

Executive Summary

This report is intended to assist the end-user of the product in determining the suitability of the product in their deployed environment.

The Target of Evaluation (TOE) is a SolarWinds Security Event Manager (SEM) v2019.4 and has undergone the CC certification procedure at the Singapore Common Criteria Scheme (SCCS). The TOE comprises of the following components:

Software
- SolarWinds Security Event Manager v2019.4

TOE preparative and operative guidance (in PDF format)
- SEM-2019-4: Installation-Guide, 29 Jul 2021
- SEM-2019-4: Admin-Guide, 29 Jul 2021
- SEM-2019-4: Getting-started-guide, 25 Feb 2020
- SEM-2019-4: Common Criteria Supplement v1.9, 3 Aug 2022

TOE is a security information and event management (SIEM) virtual appliance that provides access to log data for forensic and troubleshooting purposes, and tools to help manage log data.

TOE collects, stores, and normalizes log and event data from a variety of sources, and displays that data in a web interface for monitoring, searching, and analysis. Data is also available for scheduled and ad hoc reporting.

The evaluation of the TOE has been carried out by UL Verification Services Pte Ltd, an approved CC test laboratory at the assurance level CC EAL2, augmented by ALC_FLR.2 and completed on 12 August 2022. The certification body monitored each evaluation to ensure a harmonised procedure and interpretation of the criteria has been applied.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed Issue
Audit	Audit records are generated for any specific operations on TOE.
Identification and Authentication	Before user may access TOE function, I&A is mandatory.
Management	The management TOE security functionalities, such as assigning user role.
Log and Event Management	Manage the log and event collected from remote systems.
Secure Communication	TOE support secure protocol, such as TLS v1.2 for communication over a computer network.

Table 1: TOE Security Functionalities

Please refer to the Security Target [SolarWinds Worldwide, LLC. (2022, March 10). SolarWinds SEM Security Target v0.6.] for more information.

The assets to be protected by the TOE has been defined. Based on these assets, the TOE Security Problem Definition has been defined in terms of Assumptions, Threats and Organisation Policies. These are outlined in Chapter 3 of the Security Target.

This Certification covers the configurations of the TOE as outlined in Chapter 5.3 of this report.

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate applies only to the specific version and release of the IT product in its evaluated configuration. This certificate is not an endorsement of the IT product by SCCS, and no warranty of the IT product by SCCS, is either expressed or implied.

Table of Contents

1 Certification

1.1 Procedure

The certification body conducts the certification procedure according to the following criteria:

- Common Criteria for IT Security Evaluation (CC) Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, ISO/IEC 15408
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 5, ISO/IEC 18045
- SCCS scheme publications

1.2 Recognition Agreements

The international arrangement on the mutual recognition of certificates based on the Common Criteria Recognition Arrangement had been ratified on 2 July 2014. The arrangement covers certificates with claims of compliance against collaborative protection profiles (cPPs) or evaluation assurance levels (EALs) 1 through 2 and ALC_FLR.

Singapore is authorised to issue CC certificates recognised widely through the Common Criteria Recognition Arrangement (CCRA) by the member nations. Hence, the certification for this TOE is fully covered by the CCRA.

The Common Criteria Recognition Arrangement Logo printed on this certificate indicates that this certification is recognised under the terms of this agreement by all signatory nations listed on the CC web portal (http://www.commoncriteriaportal.org).

2 Validity of the Certification Result

This Certification Report only applies to the version of the TOE as indicated. The Certificate is valid till **1 August 2027**[1].

In cases of changes to the certified version of the TOE, the validity may be extended to new versions and releases provided the TOE sponsor applies for Assurance Continuity (i.e. re-certification or maintenance) of the revised TOE, in accordance with the requirements of the SCCS.

The owner of the Certificate is obliged:

- When advertising the Certificate or the fact of the product's certification, to refer to and provide the Certification Report, the Security Target and user guidance documentation herein to any customer of the product for the application and usage of the certified product;
- To inform the SCCS immediately about vulnerabilities of the product that have been identified by the developer or any third party; and
- To inform the SCCS immediately in the case that relevant security changes in the evaluated life cycle has occurred or the confidentiality of documentation and information related to the TOE or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is no longer valid.

[1] Certificate validity could be extended by means of assurance continuity. Certificate could also be revoked under the conditions specified in SCCS Publication 3 (Cyber Security Agency of Singapore (CSA), 2018). Potential users should check the SCCS website (https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/csa-common-criteria/product-list) for the up-to-date status regarding the certificate's validity.

3 Identification

The Target of Evaluation (TOE) is the **SolarWinds Security Event Manager v2019.4**. The following table identifies the TOE deliverables.

Type	Name	Version	Form of Delivery
SW	SolarWinds Security Event Manager	Version 2019.4	Delivered by hand
DOC	SolarWinds Security Event Manager Getting Started Guide	Version 2019.4, 25 Feb 2020	PDF format delivered via email.
DOC	SolarWinds Security Event Manager Installation Guide	Version 2019.4, 29 Jul 2021	PDF format delivered via email.
DOC	SolarWinds Security Event Manager Administrator Guide	Version 2019.4, 29 Jul 2021	PDF format delivered via email.
DOC	SolarWinds Security Event Manager Common Criteria Supplement, v1.9	Version 2019.4, 03 Aug 2022	PDF format delivered via email.

Table 2: Deliverables of the TOE

The guide for receipt and acceptance of the above-mentioned TOE are described in the set of guidance documents [2], [3], [4] and [5].

Additional identification information relevant to this Certification procedure as follows:

TOE	SolarWinds Security Event Manager (SEM) v2019.4
Security Target	SolarWinds Security Event Manager Security Target v0.6
CC Scheme	Singapore Common Criteria Scheme (SCCS)
Methodology	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5
Assurance Level	EAL 2 augmented ALC_FLR.2
Developer	SolarWinds Worldwide, LLC
Sponsor	SolarWinds Worldwide, LLC
Evaluation Facility	UL Verification Services Pte Ltd
Certification Body	Cyber Security Agency of Singapore (CSA)
Certification ID	CSA_CC_20001
Certificate Validity	**2 August 2022** till **1 August 2027**

Table 3: Additional Identification Information

4 Security Policy

The TOE's Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE.

The TOE implements policies pertaining to the following security functional classes:

- Audit
- Identification and Authentication
- Management
- Log and Event Management
- Secure Communication

Specific details concerning the above-mentioned security policies can be found in chapter 7 of the Security Target [1].

5 Assumptions and Scope of Evaluation

5.1 Assumptions

The assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE environment and are listed in the tables below

Security Objectives	Description
OE.COMM	The Operational Environment will protect communication between the TOE, SEM Agent and systems outside the TOE.
OE.ENVIRON	The Administrator will install the TOE in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.
OE.INSTALL	The Administrator will install and configure the TOE according to the administrator guidance.
OE.INTROP	The IT Systems which the TOE monitors is interoperable with the TOE
OE.NETWORK	The Administrator will install and configure a network that supports communication between TOE and other IT systems. The administrator will ensure that this network functions properly.
OE.NOEVILADMIN	Administrators are non-hostile and follow the administrator guidance when using the TOE.

Table 4: Objectives for the Operational Environment

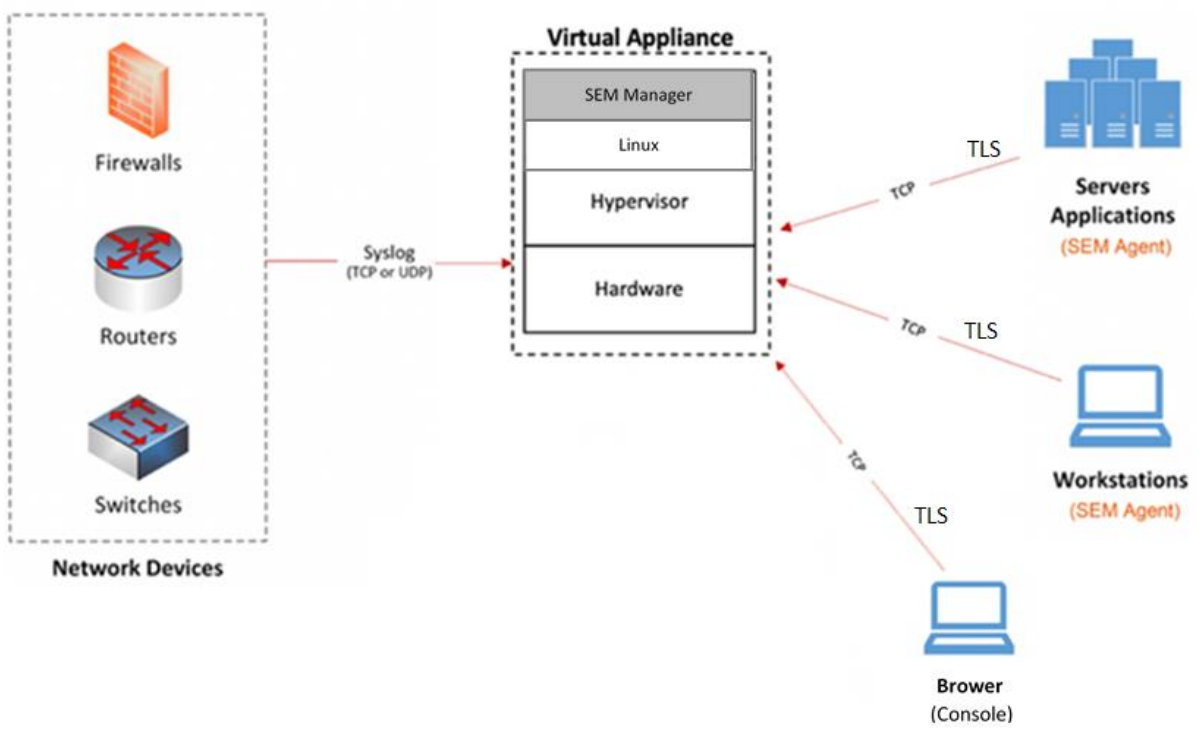
Details can be found in Section 4.2 of the Security Target [1].

5.2 Clarification of Scope

The scope of evaluation is limited to those claims made in the Security Target [1].

5.3 Evaluated Configuration

The scope of evaluation is limited to those claims made in the Security Target [1].



The Target of Evaluation is SolarWinds Security Event Manager (SEM) 2019.4. SEM is a security information and event management (SIEM) that consolidates log data for forensic and troubleshooting purposes, and tools to help manage log data.

The evaluated configuration consists of the following:

1. One instance of the SEM installed and executing on a supported hypervisor.

The following installation and configuration options must be used:

1. All User Accounts are defined as SEM Users.
2. Custom Widgets are not configured.
3. The Password Policy must be configured to require all passwords to meet complexity requirements.
4. Administrators configure passwords in accordance with the password policies for their organization.
5. The SEM is configured for log message storage and nDepth search.
6. The Enable Global Automatic Updates parameter is not set, since this could cause the TOE to be changed from the evaluated version

5.4 Non-Evaluated Functionalities

There are no non-evaluated functionalities within the scope as clarified in section 5.2.

5.5 Non-TOE Components

The TOE requires additional components (i.e. hardware/software/firmware) for its operation. These non-TOE components include:

- Hypervisor
- CPU
- Memory
- Hard Drive
- Web Browser

More information is available in Section 1.5.3 Required Non-TOE Hardware/Software/Firmware of the Security Target [1].

6 Architecture Design Information

SEM acts as a monitoring and management tool for use by network managers. It collects logs and events from multiple remote third-party systems, and alerts the network managers to specified conditions.

Users interact with the TOE via multiple mechanisms. Consoles (including SEM console, SEM event console and SEM CMC console) are provided for remote interaction with users and administrators for configuration and data access.

The TOE consists of five subsystems as follows:

1. SEM Manager
    a. SEM Manager is the essential subsystem of TOE, which support most of the TSFs, this subsystem is not directly access by TOE user, need to use consoles or report application.
2. SEM Consoles
    a. SEM Consoles provides the user access to SEM Manager to conduct TOE management and event management. When configuration changes are made, the updated information is saved and acted on.
3. SEM CMC Command Line Interface (CLI)
    a. SEM CMC command line interface (CLI) is used to establish connections to the TOE via using SSH client on a remote IT system for TOE management.
4. SEM Events Console
    a. SEM Event Console provides the user access to the SEM Manager monitoring functions from remote systems via browser sessions. It retrieves and displays the appropriate information via the browser session.
5. SEM Admin User Interface
    a. SEM Admin User Interface provides the user access to the SEM

Manager configuration functions from remote IT systems via browser sessions. This subsystem allows users to configure LDAP authentication, SSO configuration and the ability to enable/disable local SEM users.

7 Documentation

The evaluated documentation as listed in Table 2: Deliverables of the TOE is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

8 IT Product Testing

8.1 Developer Testing (ATE_FUN)

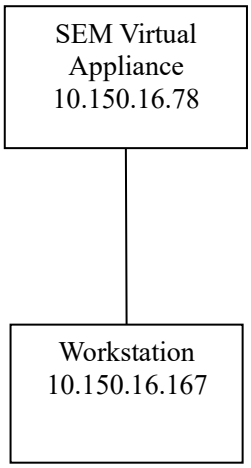
8.1.1 Test Approach and Depth

The developer has performed testing most of the interfaces. Interfaces that were not tested were included as additional test cases under ATE_IND.

8.1.2 Test Configuration

In the SEM Test Configuration, a SEM virtual appliance was deployed as a guest virtual machine running on first VMware vSphere and then Microsoft Hyper-V hypervisor hosts. The SEM virtual appliance is setup on a local area network where communication is allowed between the evaluator Workstation and the SEM Manager.

The Workstation includes a web browser and is configured to make requests via HTTPS encrypted with TLS.



An overview of the purpose of each of these systems is provided in the following table. Other systems may be present as well.

System	Purpose
SEM Virtual Appliance	SEM Virtual Appliance deployed to either VMware vSphere or Microsoft Hyper-V running SEM Manager.
Workstation	Windows 10/Windows Server 2016/2012 workstation with SEM Console installed.

8.1.3 Test Results

All test results from tested environments showed that the expected test results are identical to the actual test results.

8.2 Evaluator Testing (ATE_IND)

8.2.1 Test Approach and Depth

To gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE, the evaluator analysed the developer's test coverage, test plans and procedures, expected and actual test results.

The evaluator has repeated 4 out of 7 developer's test cases for verification purpose and determined that there are no issues.

In addition, the evaluators also devised a set of independent tests that supplements or augments developer's existing test plan to gain assurance of the security of the TOE.

8.2.2 Test Configuration

The evaluator deployed TOE as a guest virtual machine running on Microsoft Hyper-V hypervisor host. The SEM virtual appliance is setup on a local area network where communication is allowed between the evaluator's Workstation and the SEM Manager.

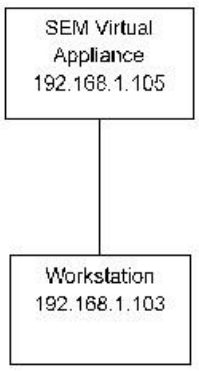


Figure 1: Environment Setup

Below table is the workstation specification.

Workstation Specifications	
Operating System	Windows Server 2016 Standard
IP Address	192.168.1.103
Web Browser	Google Chrome 92.x (64-bit)
Software Installed	• Kiwi Syslog Generator • Solar-PuTTY

Table 5: Workstation Specification

8.2.3 Test Results

The developer's test reproduced were verified by the evaluator to conform to the expected results from the test plan.

8.3 Penetration Testing (AVA_VAN)

8.3.1 Test Approach and Depth

The evaluator performed a public vulnerability search, including a literature review of conference proceedings, University research, relevant journals, published papers, any blogs and writeups. The evaluator also considered Internet surveys and online vulnerability databases. The search was executed with the following criteria:

- Product name (and variants)
- Vendor's name (and variants)
- Product type.
- Name of any components supported in the TOE operational environment or integrated in the TOE

The search provided the evaluator with a view of the vulnerabilities at the time of the TOE analysis. In combination with the search for known vulnerabilities (referred to as "public domain vulnerabilities") the evaluator performed an independent vulnerability analysis of the TOE documentation as follows:

- The security architecture of the TOE was analysed and understood based on the ARC document
- The SFRs defined in the Security Target [1] were analysed and for each, a deep understanding of the SFR was gained based on all the evidence provided for ADV.

The approach chosen by the evaluator is appropriate for the assurance component chosen (AVA_VAN.5), treating the resistance of the TOE to an attack with basic attack potential.

Test ID	Description	Remarks
Test Case #1	Self-signed certificate	This test is to analysis the possibility of exploiting the self-signed certificate.
Test Case #2	Insecure communication assessment	This is to check if network packets are sent in clear text

Test Case #3	Missing HTTP security headers assessment	This test is to check if there are missing HTTP security headers and the value in the security headers.
Test Case #4	Possible clickjacking vulnerability (Web Application Client-Side Testing)	This test is to check if SAMEORIGIN from test case 3 can be bypass and enable a clickjacking attack which will allow the attacker's page overlays the target application's interface.
Test Case #5	Adobe Flex resourceModuleURLs same-origin policy (SOP) bypass	This test is to check if SWF file with Adobe Flex application is vulnerable to Adobe Flex SDK.
Test Case #6	Default or well-known credential weakness over SSH service and proceed with restricted shell escape	This test is to check if an attacker is able to compromise the default credential and escape a restricted shell.
Test Case #7	Restricted shell escape and further local privilege escalation	The test is to check if an attacker can escape a restricted shell and perform local privilege escalation.

Table 6: Penetration Test Cases

The evaluator found no exploitable vulnerability in the TOE when operated in the evaluated configuration. Residual risk was identified, the table below shows the summary and recommendation:

Summary	Recommendation
The self-signed certificate weakness is affected to the SolarWinds SEM Events Console and SEM Admin user interface (TCP port 8443) as well as other SSL / TLS interfaces – SEM manager interfaces (TCP port 37890-37891), Secure Syslog (TCP Port 6514).	Recommended to use certificate issued by a trustworthy Certificate Authority rather than a self-signed certificate is specified in user supplement document (version 1.9).

Table 7: Residual Risk

9 Results of the Evaluation

The Evaluation Technical Report (ETR) was provided by the CCTL in accordance with the CC, CEM, requirements of the SCCS. As a result of the evaluation, the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 2 assurance package assurance package
- ALC_FLR.2

Obligations & Recommendations for Usage of the TOE

The documents as outlined in Table *2*: Deliverables of the TOE contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition, all aspects of Assumptions, Threats and OSPs as outlined in the Security Target [1] that are not covered by the TOE shall be fulfilled by the operational environment of the TOE.

Potential user of the product shall consider the results of the certification within his/her system risk management process. As attack methods and techniques evolve over time, he/she should define the period of time whereby a re-assessment of the TOE is required and convey such request to the sponsor of the certificate.

While under the developer's guidance document that "The Enable Global Automatic Updates" parameter is not to be enabled, since this could cause the TOE to be changed from the evaluated version, users are recommended to adhere to its corporate policies relating to updates and patch management.

10 Acronyms

CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CCTL	Common Criteria Test Laboratory
CSA	Cyber Security Agency of Singapore
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
PP	Protection Profile
SAR	Security Assurance Requirement
SCCS	Singapore Common Criteria Scheme
SFR	Security Functional Requirement
TOE	Target of Evaluation
TSF	TOE Security Functionality
SEM	Security Event Manager

11 Bibliography

1 SolarWinds Worldwide, LLC. (2022, March 10). SolarWinds SEM Security Target v0.6.

2 SolarWinds Worldwide, LLC. (2021, July 29). SolarWinds Security Event Manager Installation Guide v2019.4.

3 SolarWinds Worldwide, LLC. (2021, July 29). SolarWinds Security Event Manager Administrator Guide v2019.4.

4 SolarWinds Worldwide, LLC. (2020, Feburary 25). SolarWinds Security Event Manager Getting Started Guide v2019.4.

5 SolarWinds Worldwide, LLC. (2022, August 3). SolarWinds Security Event Manager Common Criteria Supplement v1.9

6 Common Criteria Maintenance Board (CCMB). (2017). Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model [Document Number CCMB-2017-04-001]. Version 3.1 Revision 5.

7 Common Criteria Maintenance Board (CCMB). (2017). Common Criteria for Information technology Security Evaluation - Part 2: Security functional components [Document Number CCMB-2017-04-002], Version 3.1 Revision 5.

8 Common Criteria Maintenance Board (CCMB). (2017). Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components [Document Number CCMB-2017-04-003], Version 3.1 Revision 5.

9 Common Criteria Maintenance Board (CCMB). (2017). Common Methodology for Information Technology Security Evaluation - Evaluation Methodology [Document Number CCMB-2017-04-004], Version 3.1 Revision 5.

10 Cyber Security Agency of Singapore (CSA). (2018, June). SCCS Publication 1 - Overview of SCCS, Version 5.0.

11 Cyber Security Agency of Singapore (CSA). (2018, June). SCCS Publication 2 - Requirements for CCTL, Version 5.0.

12 Cyber Security Agency of Singapore (CSA). (2018, June). SCCS Publication 3 - Evaluation and Certification, Version 5.0