Certification Report

SolarWinds Security Event Manager 2024.2.1

Sponsor and developer: ***SolarWinds Worldwide, LLC***
7171 Southwest Parkway Building 400
Austin, Texas 78735
USA

Evaluation facility: ***UL***
De Heyderweg, 2
Leiden, 2314XZ
The Netherlands

Report number:	**NSCIB-CC-2400076-01-CR**
Report version:	**1**
Project number:	NSCIB-**2400076-01**
Author(s):	**Alireza Rohani**
Date:	**03 February 2025**
Number of pages:	**10**
Number of appendices:	**0**

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TrustCB B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TrustCB B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TrustCB B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Recognition of the Certificate

Presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the SolarWinds Security Event Manager 2024.2.1. The developer of the SolarWinds Security Event Manager 2024.2.1 is SolarWinds Worldwide, LLC located in Austin, USA and they also act as the sponsor of the evaluation and certification A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is a security information and event management (SIEM) virtual appliance that adds value to existing security products and increases efficiencies in administering, managing, and monitoring security policies and safeguards on the network. SEM provides access to log data for forensic and troubleshooting purposes, and tools to help manage log data.

The TOE has been evaluated by UL located in Leiden, The Netherlands. The evaluation was completed on 3 February 2025 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the SolarWinds Security Event Manager 2024.2.1, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the SolarWinds Security Event Manager 2024.2.1 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL2 augmented (EAL2+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.2 (Sufficiency of security measures).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TrustCB B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the SolarWinds Security Event Manager 2024.2.1 from SolarWinds Worldwide, LLC located in Austin, USA.

To ensure secure usage a set of guidance documents is provided, together with the SolarWinds Security Event Manager 2024.2.1. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

SEM 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. SEM leverages collected logs, analyzes them in real time, and notifies problem before it causes further damage. SEM accepts normalized data and raw data from a wide variety of devices. SEM Agents (running on remote systems) normalize the data before sending the data to the SEM. Non-Agent remote devices send their log data in raw form to SEM where it is normalized by device-specific Connectors. SEM Agents are not included in the evaluation. Alerts are created from normalized data. Alerts are containers SEM uses to display events/messages from SEM monitored devices. Log data is processed by SEM’s policy engine to correlate data based on user defined Rules; when a user defined condition is detected, an Incident is created and the configured actions are initiated (when applicable). These actions can include notifying users (both locally in the Console and by email), blocking an IP address, shutting down or rebooting a workstation, and passing the alerts on to the SEM database for future analysis and reporting. Actions that are dependent upon processing by remote systems that are outside the scope of the TOE are not included in the evaluation.

2.3 Assumptions and Clarification of Scope

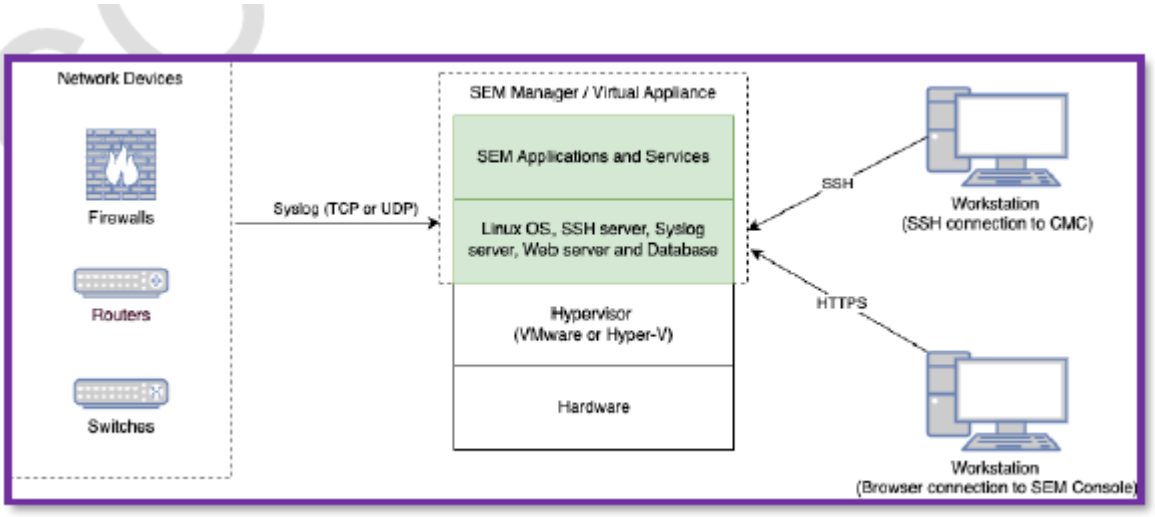
2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 3.2 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information



2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
SolarWinds Security Event Manager Getting Started Guide	V2024.2.1
SolarWinds Security Event Manager Installation Guide	V2024.2.1
SolarWinds Security Event Manager Administrator Guide	V2024.2.1
SolarWinds Security Event Manager V2024.2.1 Common Criteria Supplement	V1.4

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

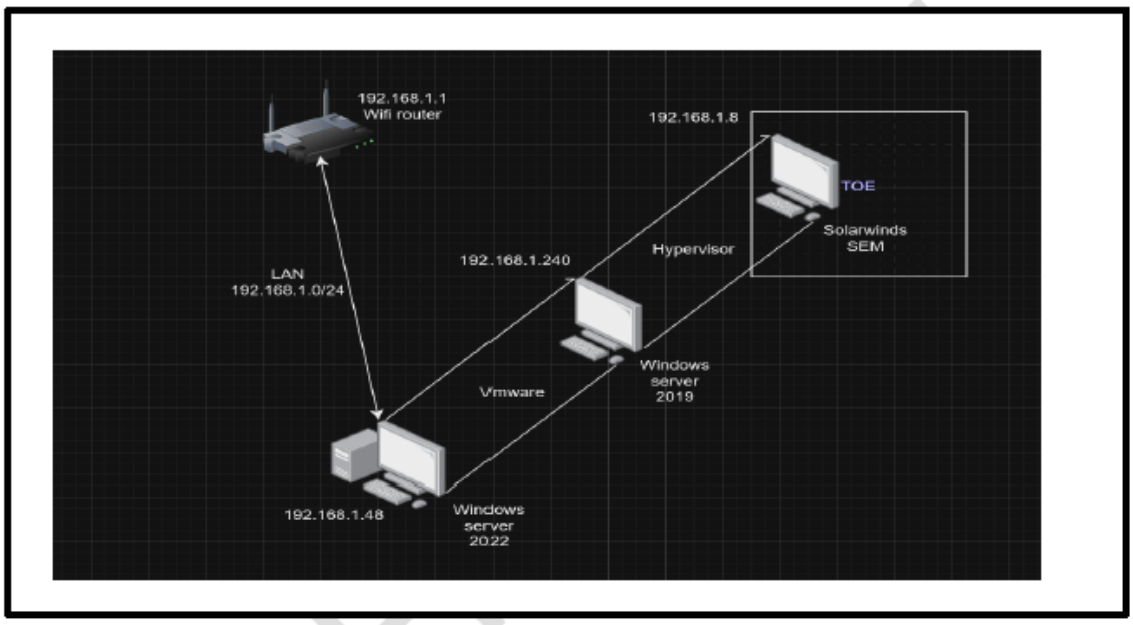
The evaluator created additional test cases test to confirm verification of the version of the TOE / to supplement coverage of SFRs and/or TSFI / to further exercise the behaviour of critical functionality.

2.6.2 Independent penetration testing

The total test effort expended by the evaluators was 1 week. During that test campaign, 100% of the total time was spent on logical tests.

2.6.3 Test configuration

The general-purpose test configuration shown in Figure below was used for all test cases described in this test results report, since the TOE has only one operational mode and the test configuration works for all the tests included in the report. The test configuration consists of the equipment listed in this section.



2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number SolarWinds Security Event Manager 2024.2.1.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the SolarWinds Security Event Manager 2024.2.1, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL2 augmented with ALC_FLR.2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: none.

3 Security Target

The Security Target for SolarWinds Security Event Manager 2024.2.1, version 1.10, 23 December 2024 *[ST]* is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

IDS	Intrusion Detection System
IP	Internet Protocol
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[ETR]	SolarWinds Security Event Manager (SEM) 2024.2.1 Evaluation Technical Report From UL TS BV UL15309535/ETR, v1.2, 09 January 2025
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[ST]	Security Target for SolarWinds Security Event Manager 2024.2.1, version 1.10, 23 December 2024

(This is the end of this report.)