# National Information Assurance Partnership

# Common Criteria Evaluation and Validation Scheme

# Validation Report

# for the

# Splunk Enterprise 8.1
# Version 1.2

| | |
|---|---|
| Report Number: | CCEVS-VR- VID 11108-2021 |
| Dated: | January 26, 2021 |
| Version: | 1.2 |

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

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

# ACKNOWLEDGEMENTS

## Validation Team

Paul Bicknell
Randy J. Heimann
Lisa Mitchell
Linda E. Morrison
Clare Olin
*The MITRE Corporation*

Farid Ahmed
Peter Kruss
*John Hopkins, APL*

## Common Criteria Testing Laboratory

Danielle Canoles

Prasad Pandit

Dayanandini Pathmanathan

Acumen Security, LLC.

## Table of Contents

# 1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Splunk Enterprise 8.1 Series Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in January2021. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Extended and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for Common Criteria for Information Technology Security Evaluations Part 1, Version 3.1, Revision 5, April 2017.

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory (CCTL) using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the Protection Profile for Application Software, Version 1.3 [SWAPP v1.3] and Functional Package for Transport Layer Security (TLS), Version 1.1 [TLS-PKG v1.1]. This VR 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 ETR are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

# 2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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). CCTLs evaluate products against PP containing Assurance Activities, which are the interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT 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 Product Compliance 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 Protection Profile(s) to which the product is conformant.
- 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** | Splunk Enterprise 8.1 |
| **Protection Profile** | Protection Profile for Application Software, Version 1.3 [SWAPP v1.3] and Functional Package for Transport Layer Security (TLS), Version 1.1 [TLS-PKG v1.1] |
| **Security Target** | Splunk Enterprise 8.1 Security Target |
| **Evaluation Technical Report** | Evaluation Technical Report for Splunk Enterprise 8.1 |
| **CC Version** | Version 3.1, Revision 5 |
| **Conformance Result** | CC Part 2 Extended and CC Part 3 Extended. |
| **Sponsor** | Splunk Inc. |
| **Developer** | Splunk Inc. |
| **Common Criteria Testing Lab (CCTL)** | Acumen Security<br>Research Blvd Suite 395<br>Rockville, MD 20850 |
| **CCEVS Validators** | Paul A Bicknell<br>Randy J Heimann |

| | |
|---|---|
| | Linda E Morrison<br>Lisa Mitchell<br>Clare Olin<br>Farid Ahmed<br>Peter Kruss |

# 3 Architectural Information

- The Target of Evaluation (TOE) is the Splunk Enterprise v8.1 which runs on Red Hat Linux Enterprise (RHEL) v7.7 and v8.2 operating systems. Splunk collects data from various sources such as systems, devices, and interactions and presents the data for real time visibility and analysis. The TOE can be configured as a forwarder and an indexer. When the TOE is configured as the indexer, it will receive data from external sources such as web services, databases, and one or more instance of Splunk configured as a Forwarder. In Forwarder configuration, it will transmit all system generated data to the other instance of Splunk configured as an Indexer.
- The TOE is a software application running on Dell PowerEdge R430 Server with Intel Xeon E5-2630 v4 (Broadwell) processor, and it includes 1TB disk and 32GB RAM. The TOE is Splunk Enterprise v8.1 which runs on Red Hat Linux Enterprise (RHEL) v7.7 and v8.2 64-bit operating system.

# 4 Security Policy

### Logical Scope of the TOE

The TOE provides the security functionality required by [SWAPP] and [TLS v1.1 package] as listed below:

## 4.1 Cryptographic Support

The TOE platform provides HTTPS/TLS functionality to securely communicate with trusted entities. TOE is shipped with the OpenSSL which performs the TOE's cryptographic operations. TOE leverages the services of the underlying platform to generate entropy for deterministic random bit generator and key store to store the key data.

The following table contains the CAVP algorithm certificates:

| Algorithm | Related SFRs | Description | Modes Supported | CAVP Certificate # |
|---|---|---|---|---|
| AES | FCS_COP.1(1) | Used for Symmetric Encryption/Decryption | GCM (256,128),<br>CBC (256) | C1827<br>C1828 |
| DRBG | FCS_RBG_EXT.1.1 | Deterministic random bit generation | CTR_DRBG AES | C1827<br>C1828 |
| ECDSA | FCS_CKM_EXT.1.1<br>FCS_COP.1(3)<br>FCS_CKM.2 | 186-4 Key Pair Generation and Private Key Validation<br>Signature Generation and Signature Verification<br>ECC Key Establishment | P-256, P-384 and P-521 | C1827<br>C1828<br>A878<br>A879 |
| HMAC | FCS_COP.1(4) | Keyed-Hash Message Authentication | HMAC-SHA-256 and HMAC-SHA-384 | C1827<br>C1828 |
| SHS | FCS_COP.1(2) | Cryptographic Hashing Services | SHA-256, SHA-384 and SHA-512 | C1827<br>C1828 |

**Table 3 CAVP Certificate References**

## 4.2 User Data Protection

The TOE is installed on the encrypted partition of the underlying host platform to secure its data. The private key data for the certificates is stored on the secret storage that can be accessed with the password set to encrypt the partition. Prior to the installation of TOE, the hard drive on the host machine should be encrypted using LUKS. The TOE depends on the underlying platform's network connectivity for its management purpose, sending email alerts to the SMTP server and sending data to the external trusted data feed receiver (TOE Indexer) or receiving the data from the external trusted data feed (TOE Forwarder).

## 4.3 Identification and Authentication

The TOE relies on X.509v3 certificate validation functions provided by the platform to authenticate the certificate(s) during the establishment of the HTTPS/TLS trusted channel. If the certificate is found to be invalid the TOE rejects such certificate. Certificate with the unknown revocation status is accepted if the TOE is unable to validate the certificate through CRL.

## 4.4 Security Management

The TOE is not shipped with the default credentials used for the Initial authentication. Once the TOE is installed on the RHEL server all the directories and configuration files that are related to the TOE are protected and has the write access to only the user that performed the installation. The TOE has several configuration files that makes communication possible between the other network entities. An administrator can configure the supported TLS cipher suites and curves in these files for the secure communication with the entities and can also query the TOE version.

## 4.5 Privacy

The TOE does not request any personally identifiable information (PII) with the intent to transmit the data over the network, thus maintaining privacy of the security administrators and the users.

## 4.6 Protection of the TSF

The TOE’s platform performs cryptographic self-tests at startup which ensures the TOE’s ability to properly operate. The updates must be downloaded manually and installed using the platform’s package manager. The TOE platform also verifies all software updates via digital signature wherein the administrator must install the public key of the TOE's developer to check the integrity of any available updates. The TOE uses platform APIs and includes only 3rd party libraries. It also implements stack-based buffer overflow protection along with ASLR (address space layout randomization) and allocating memory for both writing and execution for just-in-time compilation. The TOE supports SElinux and is one of the pre-requisites before installing the TOE application.

## 4.7 Trusted Path/Channels

The TOE is a software application. It supports HTTPS/TLS for secure remote administration communication for WebUI. HTTPS/TLS is used for secure communication channel between the TOE indexer and external trusted data feeds (TOE Forwarder), the TOE acting as an Indexer uses TLS to securely send email alerts to a remote SMTP server. The TOE when configured as a Forwarder uses HTTPS/TLS for sending data to an external data feed receiver (TOE Indexer).

# 5 Assumptions, Threats, and Clarification of Scope

## 5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

The following assumptions are drawn directly from the [SWAPP]:

| ID | Assumption |
|---|---|
| A.PLATFORM | The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE. |
| A.PROPER_USER | The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy. |
| A.PROPER_ADMIN | The administrator of the application software is not careless, willfully negligent, or hostile, and administers the software in compliance with the applied enterprise security policy. |

**Table 2 Assumptions**

## 5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment.  The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

The following threats are drawn directly from the [SWAPP]:

| ID | Threat |
|---|---|
| T.NETWORK_ATTACK | An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it. |
| T.NETWORK_EAVESDROP | An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints. |
| T.LOCAL_ATTACK | An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications. |
| T.PHYSICAL_ACCESS | An attacker may try to access sensitive data at rest. |

**Table 3 Threats**

### 5.3 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:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the Protection Profile for Application Software, Version 1.3 [SWAPP v1.3] and Functional Package for Transport Layer Security (TLS), Version 1.1 [TLS-PKG v1.1].
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
- Consistent with the expectations of the PP, 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.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.
- The TOE must be installed, configured, and managed as described in the documentation referenced in section 6 of this Validation Report.

# 6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Splunk Enterprise v8.1 Common Criteria Guide v0.9 [AGD]

# 7 TOE Evaluated Configuration

## 7.1 Evaluated Configuration

The TOE is the Splunk Enterprise v8.1 which is executed on RHEL operating system. The Splunk Enterprise is a software application that enables users to search, analyze, and visualize the data that is gathered from various components of an IT infrastructure or business industry. The evaluated version of the TOE is v8.1.

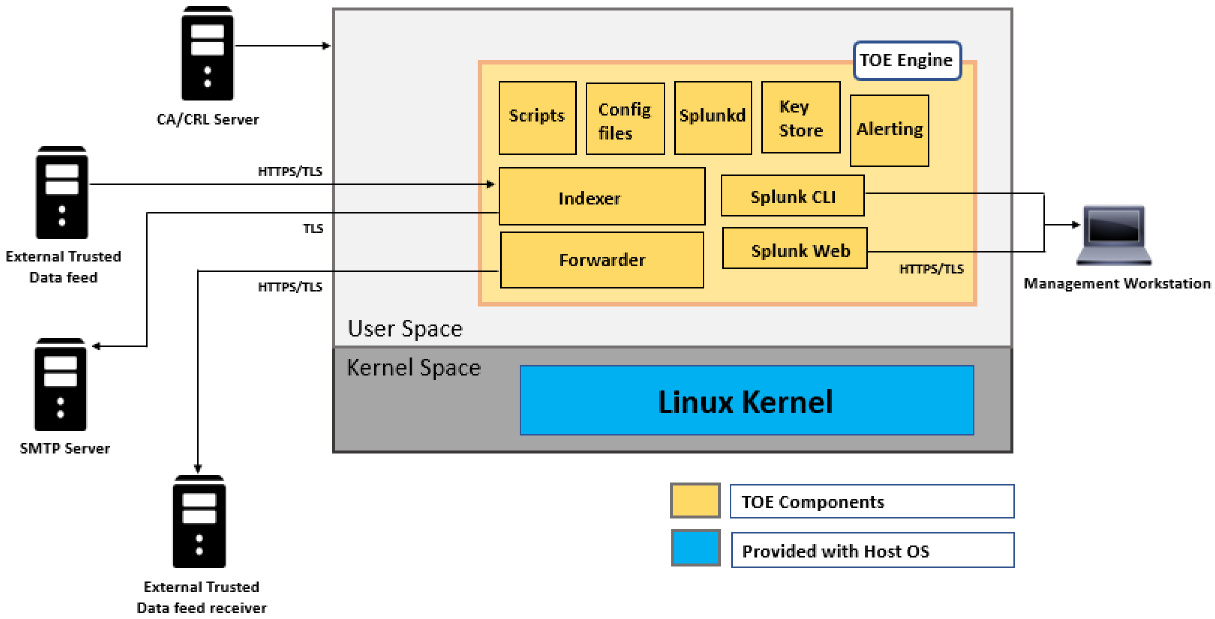

**Figure 1: TOE Boundary Diagram**

As noted in Figure 1, The TOE consists of many components: Splunkd, Splunk CLI, Splunk Web, Splunk Scripts, Splunk alerts, Splunk KeyStore and Splunk config files. Splunkd is the system process that handles indexing, searching, forwarding, and the Web interface that the user logs into Splunk Enterprise. The above Figure also shows the TOE uses the underlying host platform for storing the Scripts, Key store and Config files which are considered part of the application.

Splunk Web is the web-based user interface for the Splunk to manage the application using a graphical interface. The user logs into Splunk web interface with any supported browser. The communication between the browser and the Splunk Web is over HTTPS/TLS. An administrator must authenticate to Splunk Web using the username and password.

Splunkd is the system process that handles indexing, searching, forwarding, and the Web interface that the user logs into Splunk Enterprise. In order to start this process, the administrator must start the application by using the command "start splunk" in the application directory.

Splunk CLI provides a command line interface that is used to manage the application locally. The CLI service is provided by the underlying host platform. It is mainly used to navigate to the application directories and run the Splunk specific commands. It has the same functionality as Splunk Web except for the graphical representation.

Splunk alerts are actions which gets triggered when a specific criterion is met which is defined by the user. Different types of alerts can be configured in Splunk. In this evaluation email alerts are configured that sends an email to the SMTP server when an action is triggered.

Splunk Scripts can be created to automate the Splunk functionality, an administrator can create simple scripts to start and stop the Splunk application.

Splunk KeyStore is mainly used to store the data for keys, the KeyStore is accessed using the Gnome keyring. Splunk requires at least two partitions of the underlying platform to be LUKS encrypted.

Splunk Enterprise configuration settings are stored in configuration files. These files are available on Splunk with an extension .conf and are easily readable and editable if the user has appropriate access. Below is the list of Splunk configuration files:

- inputs.conf
- outputs.conf
- server.conf
- alert_actions.conf
- web.conf

In the evaluated configuration the TOE is configured to act as both Indexer and Forwarder.

Splunk Indexer is a Splunk instance that is installed on the physical Red Hat Enterprise Server and is configured to receive the data from the Splunk Forwarder instance. The communication between the Indexer and the Forwarder is over HTTPS/TLS.

Splunk Indexer also communicates with SMTP server for sending email alerts, the communication between the Indexer and the SMTP server is over HTTPS/TLS.

Splunk Forwarder is a Splunk instance that is installed on the physical Red Hat Enterprise Server and is configured to send the data to the Splunk Indexer instance. The communication between the Forwarder and the Indexer is over HTTPS/TLS.

The external trusted data feed is an external data source for transmitting non-TSF related data to the TOE Indexer for populating Splunk's datastore.

The external trusted data feed receiver is an external data source for receiving non-TSF related data from the TOE Forwarder for populating Splunk's datastore.

In the evaluated configuration, the software was installed on the following hardware:

- Dell PowerEdge R430 Server with Intel Xeon E5-2630 v4 (Broadwell)

Note: The TOE is the application software only. The host platforms are not part of the evaluation.

The TOE supports secure connectivity with several other IT environment devices as described below:

| Component | Required | Usage/Purpose Description |
|---|---|---|
| External Trusted Data Feed | Yes | External data source for transmitting non-TSF related data to the TOE indexer for populating Splunk's datastore. The external data source must use HTTPS/TLS to communicate with the TOE. |
| External Trusted Data Feed Receiver | Yes | External data source for receiving non-TSF related data from the TOE forwarder. The external data source must use HTTPS/TLS to communicate with the TOE. |
| Host Platform | Yes | A general-purpose computer on which the RHEL operating system and the TOE is installed. |
| Management Workstation | Yes | Used to remotely manage the TOE via HTTPS/TLS interface. |
| SMTP Server | Yes | External data source for receiving non-TSF related data from the TOE Indexer. The external data source must use HTTPS/TLS to communicate with the TOE. |
| CRL Server | Yes | Server which contains updated revocation list for the TOE. |

**Table 5 IT Environment Components**

## 7.2 Excluded Functionality

The following components are included with the Splunk Enterprise v8.1 product but are separately licensed and not considered to be within the TOE boundary:

- Data Fabric Search

Functionality or components that are part of the product but are not part of the TOE relevant functionality are listed below:

- HTTPS administrative interface – port 8089
- The KV store service, port 8191
- The TOE's ability to search and index information is not part of the evaluation. However, the data is needed in order to stimulate events for testing PP related functionality.

# 8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for Splunk Enterprise 8.1, which is not publicly available. The AAR provides an overview of testing and the prescribed assurance activities.

## 8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

## 8.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the Protection Profile for Application Software, Version 1.3 [SWAPP v1.3] and Functional Package for Transport Layer Security (TLS), Version 1.1 [TLS-PKG v1.1]. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

# 9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that activities and work units received a passing verdict.

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 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Splunk Enterprise 8.1 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in the SWAPP v1.3 and TLS-PKG v1.1.

## 9.1 Evaluation of Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Splunk Enterprise 8.1 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the Protection Profile for Application Software, Version 1.3 [SWAPP v1.3] and Functional Package for Transport Layer Security (TLS), Version 1.1 [TLS-PKG v1.1].

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 9.2 Evaluation of Development Documentation (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the Protection Profile for Application Software, Version 1.3 [SWAPP v1.3] and Functional Package for Transport Layer Security (TLS), Version 1.1 [TLS-PKG v1.1]. related to the examination of the information contained in the TOE Summary Specification.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

## 9.3 Evaluation of Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the Protection Profile for Application Software, Version 1.3 [SWAPP v1.3] and Functional Package for Transport Layer Security (TLS), Version 1.1 [TLS-PKG v1.1]. related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

## 9.4 Evaluation of Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was adequately identified.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 9.5 Evaluation of Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the Protection Profile for Application Software, Version 1.3 [SWAPP v1.3] and Functional Package for Transport Layer Security (TLS), Version 1.1 [TLS-PKG v1.1]. and recorded the results in a Test Report, summarized in the ETR and AAR.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the Protection Profile for Application Software, Version 1.3 [SWAPP v1.3] and Functional Package for Transport Layer Security (TLS), Version 1.1 [TLS-PKG v1.1] and that the conclusion reached by the evaluation team was justified.

## 9.6 Vulnerability Assessment Activity (AVA)

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities on 03rd July 2020, 04th September 2020, 11th November 2020, 30th November 2020, and 14th January 2021 and did not discover any issues with the TOE. The terms used for the search were as follows:

- Splunk
- Splunk 8.1
- Splunk 8.1.1
- TCP
- UDP
- X509
- TLS 1.2
- IPV4
- OpenSSL 1.0.2k-fips
- OpenSSL 1.0.2u-fips
- application software
- splunkd
- Intel Xeon Broadwell
- OpenSSL 1.0.2k-fips
- openssl
- Redhat
- Intel Xeon
- CherryPy
- RHEL 7.7
- RHEL 8.2

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the Protection Profile for Application Software, Version 1.3 [SWAPP v1.3] and Functional Package for Transport Layer Security (TLS), Version 1.1 [TLS-PKG v1.1], and that the conclusion reached by the evaluation team was justified.

## 9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the Protection Profile for Application Software, Version 1.3 [SWAPP v1.3] and Functional Package for Transport Layer Security (TLS), Version 1.1 [TLS-PKG v1.1], and correctly verified that the product meets the claims in the ST.

## 10 Validator Comments and Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Splunk Enterprise v8.1 Common Criteria Guide v0.9. No versions of the TOE and software, either earlier or later were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the SMTP server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

# 11 Annexes

Not applicable.

# 12 Security Target

ST Reference: Splunk Enterprise v8.1 Security Target v2.8 [ST]

# 13 Glossary

The following definitions are used throughout this document:

- **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 for Information Technology Security Evaluation - Part 1: Introduction and General Model, Version 3.1 Revision 5, April 2017.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5, April 2017.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5, April 2017.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
5. Protection Profile for Application Software, Version 1.3, dated 01 March 2019 [SWAPP]
6. Functional Package for Transport Layer Security (TLS), Version 1.1, dated 01 March 2019 [TLS-PKG]
7. Splunk Enterprise 8.1 Security Target, Version 2.8, January 28, 2021 [ST]
8. Splunk Enterprise 8.1 Common Criteria Configuration Guide, Version 0.9, January 21, 2021 [AGD]
9. Assurance Activity Report for Splunk Enterprise 8.1, Version 1.4, January 25, 2021 [AAR]
10. Vulnerability Assessment for Splunk Enterprise 8.1, Version 1.8, January 14, 2021 [AVA]
11. Evaluation Technical Report for Splunk Enterprise 8.1, Version 1.3, January 21, 2021 [ETR]
12. Test Report for Splunk Enterprise 8.1 (v7.7), Version 1.0, January 20, 2021
13. Test Report for Splunk Enterprise 8.1 (v8.2), Version 1.1, January 21, 2021