National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Axonius Cybersecurity Asset Management Platform v4.0-f

Report Number:	**CCEVS-VR-VID11201-2022**
Dated:	**3 March 2022**
Version:	**1.0**

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

<u>Validation Team</u>

Sheldon Durrant
Lisa Mitchell
Linda Morrison
Clare Parran
The MITRE Corporation

<u>Common Criteria Testing Laboratory</u>

Leidos Inc.
Columbia, MD

Contents

List of Tables

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Axonius Cybersecurity Asset Management Platform v4.0-f (the Target of Evaluation, or 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 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 in 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 evaluated and tested and any restrictions on the evaluated configuration. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST. 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.

The evaluation was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in March 2022. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report written by Leidos. The evaluation determined that the TOE is Common Criteria Part 2 Extended and Common Criteria Part 3 Extended and meets the assurance requirements of the following documents:

- *Protection Profile for Application Software*, Version 1.3, 1 March 2019 ([5])
- *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 12 February 2019 ([6])
- *Extended Package for Secure Shell (SSH)*, Version 1.0, 19 February 2016 ([7]).

The TOE is Axonius Cybersecurity Asset Management Platform v4.0-f.

The TOE identified in this VR has been evaluated at a NIAP approved 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). The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The validation team monitored the activities of the evaluation 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 the evaluation demonstrated the product satisfies all of the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) specified in the ST. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct.

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profile, Functional Package, and Extended Package, and when installed, configured and operated as described in the evaluated guidance documentation, satisfies all the SFRs specified in the ST ([8]).

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria (CC) and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of 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 Compliant List (PCL).

Table 1 provides information needed to completely identify the product, including:

- The TOE—the fully qualified identifier of the product as evaluated
- The ST—the unique identification of the document describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The PP/PP-Modules 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	Axonius Cybersecurity Asset Management Platform v4.0-f
Security Target	Axonius Cybersecurity Asset Management Platform v4.0-f Security Target, Version 1.0, 3 February 2022
Sponsor & Developer	Axonius Federal Systems LLC 10010 Junction Dr Suite No. 102-S Annapolis Junction, MD 20701
Completion Date	March 2, 2022
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM Version	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
PP	• *Protection Profile for Application Software*, Version 1.3, 1 March 2019 ([5]) • *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 12 February 2019 ([6]) • *Extended Package for Secure Shell (SSH)*, Version 1.0, 19 February 2016 ([7]).
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 extended

Item	Identifier
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Evaluation Personnel	Anthony Apted Pascal Patin Furukh Siddique
Validation Personnel	Sheldon Durrant Lisa Mitchell Linda Morrison Clare Parran

3 TOE Architecture

Note: The following architectural description is based on the description presented in the ST.

The TOE is a Linux-based containerized software application written in Python (both versions 2 and 3) and includes the Python Cryptography library that uses CAVP validated OpenSSL FIPS Object Module (FOM) for its cryptographic functionality. JavaScript version ES6 is used for the web app's front end and nginx as its web server. The embedded Python Paramiko module is used for the SSHv2 implementation. The embedded Python Secrets module provides random number generation services. The TOE includes a MongoDB database running within its own Docker container for secure storage of credentials. Both modules and the database use the FOM for cryptographic primitives. The FOM is included with the TOE.

Axonius integrates with numerous security and management solutions or assets on a network that are referred to as adapter data sources. Outbound connections to data sources are secured using HTTPS or SSH. In the evaluated configuration, unsecured connections to data sources should not be used. All management of the TOE is done through the GUI, which is protected by HTTPS/TLS.

The TOE is supported on a Ubuntu Linux-based virtualized appliance platform with Linux Unified Key Setup (LUKS) and uses Docker to run its containerized applications. In the evaluated configuration, the TOE runs on a virtual machine with Ubuntu 16.04 and Docker runtime engine v19.0.3 on ESXi 6.5 on AMD Ryzen Threadripper 1950X (Zen microarchitecture).

4 Security Policy

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

Note: Much of the description of the security policy has been derived from the ST and the Final ETR.

4.1 Cryptographic Support

The TOE implements cryptography to protect data at rest and in transit.

For data at rest, the TOE securely stores the credential data used to log in to the TOE, private keys, and the credentials the TOE uses to authenticate to adapter data sources. This stored data is protected using either PBKDF2_HMAC with SHA512 and 100,000 rounds in conjunction with LUKS or using MongoDB's Client-Side Field Level Encryption (AES-256-CBC).

For data in transit, the TOE implements HTTPS and TLS as both a client and a server. The TOE implements a HTTPS/TLS server for its administrative interface, while it implements either an SSH Client or a HTTPS/TLS client to communicate with any data sources connected to it. The TOE does not support mutual authentication.

The TOE implements all cryptography used for these functions using its own OpenSSL with CAVP validated algorithms. The TOE's DRBG is seeded using entropy from the underlying OS platform.

4.2 User Data Protection

The TOE protects sensitive data in non-volatile memory using approved cryptographic algorithms and by leveraging LUKS functionality provided by the host platform.

The TOE relies on the network connectivity capabilities of its host OS platform. The TOE supports user-initiated and application-initiated uses of the network.

The TOE does not access any of the sensitive information repositories on the host platform.

4.3 Identification and Authentication

The TOE supports X.509 certificate validation as part of establishing TLS and HTTPS connections. The TOE supports various certificate validity checks and checks certificate revocation status using OCSP. If the certificate is invalid or the revocation status of a certificate cannot be determined, the certificate will not be accepted.

4.4 Security Management

The TOE itself and the configuration settings it uses are stored in locations recommended by the Linux platform vendor.

The TOE includes a web GUI. This interface enforces username/password authentication using locally stored credentials that are created using the TOE. The TOE does not include a default user account to access its management interface.

The security-relevant management functions supported by the TOE relate to configuration of adapters and certificates.

4.5 Privacy

The TOE does not collect or transmit personally identifiable information (PII) of any individuals.

4.6 Protection of the TSF

The TOE enforces various mechanisms to prevent itself from being used as an attack vector to its host OS platform. The TOE runs on top of the host operating system as a series of Docker containers containing Python and JavaScript code, and does not explicitly require disabling built-in operating system controls for any reason (e.g., those built into Ubuntu 16.04). As such, the TOE relies on the operating system to handle sensitive low-level operations such as memory mapping, and is compatible with Ubuntu 16.04, including when SELinux is enabled on the host OS. The TOE is interpreted code and not just-in-time compiled and therefore compiler flags to enforce ASLR are not necessary. The TOE also does not use both PROT_WRITE and PROT_EXEC on the same memory regions. There is no situation where the TSF maps memory to an explicit address.

The TOE does not use any undocumented platform APIs and no system calls are directly invoked in Axonius code. The TOE is entirely Dockerized Python/JavaScript, so all calls are indirect.

The TOE has a mechanism to determine its current software version. Software updates to the TOE can be acquired by leveraging its OS platform. All updates are digitally signed to guarantee their authenticity and integrity.

The TOE developer has internal mechanisms for receiving reports of security flaws, tracking product vulnerabilities, and distributing software updates to customers in a timely manner.

4.7 Trusted Path/Channels

The TOE encrypts sensitive data in transit between itself and its operational environment using TLS, HTTPS, or SSH.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The ST references the PP to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PP, are as follows:

- 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.
- The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
- 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.

5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the PPs listed under Identification, as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

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 shows only that the evaluated configuration meets the security claims made, with a certain level of assurance, achieved through performance by the evaluation team of the evaluation activities specified in the following documents:
  - *Protection Profile for Application Software*, Version 1.3, 1 March 2019 ([5])
  - *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 12 February 2019 ([6])
  - *Extended Package for Secure Shell (SSH)*, Version 1.0, 19 February 2016 ([7])
- This evaluation covers only the specific software distribution and version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in Axonius Cybersecurity Asset Management Platform v4.0-f Security Target, Version 1.0, 3 February 2022 ([8]). Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality mentioned in Section 8.2 of this document is excluded from the scope of the evaluation.
- This evaluation did not specifically search for, nor attempt to exploit, 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 TOE must be installed, configured and managed as described in the documentation referenced in Section 6 of this VR.

6 Documentation

The vendor offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation and delivered with the TOE is as follows:

- *Axonius Cybersecurity Asset Management Platform v4.0-f Common Criteria Evaluated Configuration Guide (CCECG)*, Version 1.0, 14 January 2022 ([9])

To use the product in the evaluated configuration, the product must be configured as specified in this documentation.

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the TOE as evaluated. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

7 IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following proprietary document:

- *Axonius Common Criteria Test Report and Procedures*, Version 1.1, 22 February 2022 ([14])

A non-proprietary description of the tests performed and their results is provided in the following document:

- *Assurance Activities Report for Axonius Cybersecurity Asset Management Platform v4.0-f*, Version 1.0, 28 February 2022 ([13])

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to the following specifications:

- *Protection Profile for Application Software*, Version 1.3, 01 March 2019
- *Functional Package for Transport Layer Security (TLS)*, Version 1.1, February 12, 2019
- *Extended Package for Secure Shell (SSH)*, Version 1.0, February 19, 2016

The evaluation team devised a test plan based on the test activities specified in these documents. The test plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the test plan and documented the results in the team test report listed above.

Independent testing took place at Leidos CCTL facilities in Columbia, Maryland, from June 2021 through February 2022.

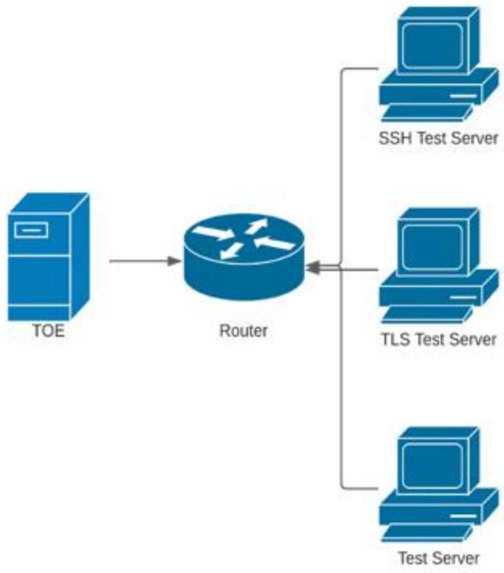
The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the team test plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for *Protection Profile for Application Software*, *Functional Package for Transport Layer Security (TLS)*, and *Extended Package for Secure Shell (SSH)* were fulfilled.

7.1 Test Configuration

The evaluation team established a test configuration comprising one instance of the TOE as follows: Axonius Cybersecurity Asset Management Platform v4.0.11-f. A schematic of the test configuration is presented in Figure 1 below.

Figure 1: TOE Test Configuration



The test configuration included the following devices in the operational environment of the TOE:

- TOE platform—execution environment for the TOE, comprising:
  - Docker runtime engine v19.0.3
  - Ubuntu 16.04
  - VMware ESXi 6.5
  - AMD Ryzen Threadripper 1950X (Zen microarchitecture) processor
- Test Server—used for general testing and collection of test artifacts. It included the following software:
  - Ubuntu 20.04
  - Sslyze v5.0.0
- TLS Server/OCSP Responder—used to test TLS client, TLS server, X.509 requirements. It included the following software:
  - Ubuntu 18.04.1
  - OpenSSL v1.1.1
  - Wireshark v2.6.1.0
  - XCA v1.3.2
  - Nmap v7.6
  - Hex Editor v1.2.13
  - CCTL's custom TLS Server and TLS Client test tools
- SSH Server—used to test SSH client. It included the following software:
  - Ubuntu 16.04.7
  - OpenSSH v7.2p2
  - Wireshark v2.6.1.0.

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The specific tested version was 4.0.11-f. The TOE consists of exactly one instance of Axonius Cybersecurity Asset Management Platform v4.0-f provided as either a .deb file or a .deb file packaged as an OVA file, executing on a platform consisting of:

- Docker runtime engine v19.0.3
- Ubuntu Linux 16.04
- VMware ESXi 6.5
- AMD Ryzen Threadripper 1950X (Zen microarchitecture) processor.

In addition to the execution platform identified above, the TOE's operational environment includes:

- A web browser, used to access the management web GUI (Chrome v84 and Firefox v79 are vendor-tested)
- One or more adapter data sources as identified in Appendix B of the ST.

8.2 Excluded Functionality

The following features and capabilities of Axonius Cybersecurity Asset Management Platform v4.0-f are not covered by the evaluation:

- The TOE's data collection, analysis, and automated response capabilities (aside from the trusted channels used to communicate with assets)
- Any other product behavior not explicitly specified and described in the claimed PP and associated packages.

9 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary Evaluation Technical Report for Axonius Cybersecurity Asset Management Platform v4.0-f ([10]). The reader of this VR can assume that all assurance activities and work units received passing verdicts.

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, revision 5 ([1], [2], [3]) and CEM version 3.1, revision 5 ([4]), and the specific evaluation activities specified in:

- *Protection Profile for Application Software*, Version 1.3, 1 March 2019 ([5])
- *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 12 February 2019 ([6])
- *Extended Package for Secure Shell (SSH)*, Version 1.0, 19 February 2016 ([7])

The evaluation determined the TOE satisfies the conformance claims made in the Axonius Cybersecurity Asset Management Platform v4.0-f Security Target, of Part 2 extended and Part 3 extended. The TOE satisfies the requirements specified in the PP and associated packages listed above.

The Validators reviewed all the work of the evaluation team and agreed with their practices and findings.

9.1 Evaluation of the Security Target (ST) (ASE)

The evaluation team performed each TSS evaluation activity and ASE CEM work unit. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description, security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements claimed to be met by the product that are consistent with the claimed PP, and security function descriptions that satisfy the requirements.

9.2 Evaluation of the Development (ADV)

The evaluation team performed each ADV evaluation activity and applied each ADV_FSP.1 CEM work unit. The evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed PP for design evidence. The ADV evidence consists of the TSS descriptions provided in the ST and product guidance documentation providing descriptions of the TOE external interfaces.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team performed each guidance evaluation activity and applied each AGD work unit. The evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was complete.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team performed each ALC evaluation activity and applied each ALC_CMC.1 and ALC_CMS.1 CEM work unit, to the extent possible given the evaluation evidence required by the claimed PP. The evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence, and that the ST describes how timely security updates are made to the TOE.

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

The evaluation team performed each test activity and applied each ATE_FUN.1 CEM work unit. The evaluation team ran the set of tests specified by the claimed PP and recorded the results in the Test Report, summarized in the AAR.

9.6 Vulnerability Assessment Activity (AVA)

The evaluation team performed each AVA evaluation activity and applied each AVA_VAN.1 CEM work unit. The evaluation team performed a vulnerability analysis following the processes described in the claimed PP. This comprised a search of public vulnerability databases.

The evaluation team performed a search of the National Vulnerability Database (https://nvd.nist.gov/).

The evaluation team initially performed searches on 14 January 2022 and repeated those searches on 8 February 2022. The evaluation team performed final searches, including new search terms suggested by the validators, on 28 February 2022, using the following search terms:

- “axonius”
- “asset management platform”
- “mongodb 4.2.8”
- “openssl 1.0.2”
- “python”
- “tls 1.2”
- “paramiko ssh”
- “esxi 6.5”
- “ubuntu 16.04”
- “docker 19.03”.

The results of these searches did not identify any vulnerabilities that are applicable to the TOE. The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

9.7 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met, sufficient to satisfy the assurance activities specified in the claimed PP. Additionally, the evaluation team’s testing 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 followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the SFRs specified in the Security Target, and the only evaluated functionality was that which was described by the SFRs claimed in the Security Target. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained.

The validators note that rekeying of SSH sessions will not occur because the transactions performed over SSH are so short that they will never reach the time and data thresholds mandated by *Extended Package for Secure Shell (SSH)*, Version 1.0, 19 February 2016 ([7])

The validators note that, because the TOE runs in a Docker container, dynamic libraries are not installed in the typical location.

11 Security Target

The ST for this product's evaluation is *Axonius Cybersecurity Asset Management Platform v4.0-f Security Target*, Version 1.0, 3 February 2022 ([8]).

12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
cPP	collaborative Protection Profile
ETR	Evaluation Technical Report
FOM	FIPS Object Module
GUI	Graphical User Interface
IT	Information Technology
LUKS	Linux Unified Key Setup
PCL	Product Compliant List
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
VM	Virtual Machine
VR	Validation Report

13 Bibliography

The validation team used the following documents to produce this VR:

[1] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security assurance requirements, Version 3.1, Revision 5, April 2017.

[4] Common Criteria Project Sponsoring Organisations. Common Evaluation Methodology for Information Technology Security, Version 3.1, Revision 5, April 2017.

[5] Protection Profile for Application Software, Version 1.3, 1 March 2019.

[6] Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019.

[7] Extended Package for Secure Shell (SSH), Version 1.0, 19 February 2016.

[8] Axonius Cybersecurity Asset Management Platform v4.0-f Security Target, Version 1.0, 3 February 2022.

[9] Axonius Cybersecurity Asset Management Platform v4.0-f Common Criteria Evaluated Configuration Guide (CCECG), Version 1.0, 14 January 2022.

[10] Evaluation Technical Report for Axonius Cybersecurity Asset Management Platform v4.0-f, Version 1.0, 28 February 2022.

[11] Assurance Activities Report for Axonius Cybersecurity Asset Management Platform v4.0-f, Version 1.0, 28 February 2022.

[12] Axonius Common Criteria Test Report and Procedures, Version 1.1, 22 February 2022.