MINISTRY OF DIGITAL

CyberSecurity MALAYSIA

C138 Certification Report

Cohesity DataProtect Version 7.1.2

File name: ISCB-3-RPT-C138-CR-v1
Version: v1
Date of document: 18 September 2024
Document classification : PUBLIC

For general inquiry about us or our services,
please email: mycc@cybersecurity.my

C138 Certification Report

Cohesity DataProtect Version 7.1.2

18 September 2024

ISCB Department

CyberSecurity Malaysia

Level 7, Tower 1,
Menara Cyber Axis, Jalan Impact,
63000 Cyberjaya, Selangor, Malaysia
Tel: +603 8800 7999 □ Fax: +603 8008 7000
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C138 Certification Report
DOCUMENT REFERENCE:	ISCB-3-RPT-C138-CR-v1
ISSUE:	v1
DATE:	18 September 2024
DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 7, Tower 1

Menara Cyber Axis

Jalan Impact

63000 Cyberjaya

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 201601006881 (726630-U)

Printed in Malaysia

Foreword

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order 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 satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 25 September 2024, and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) https://iscb.cybersecurity.my/index.php/certification/product-certification/mycc/ and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme using the Common Methodology for IT Security Evaluation, version 3.1 revision 5 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 5 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	30 August 2024	All	Initial draft
v1	18 September 2024	All	Document has been reviewed by evaluator and developer

Executive Summary

The Target of Evaluation (TOE) is Cohesity DataProtect Version 7.1.2. The TOE is a software suite that is used to hyperconverged secondary storage workloads (i.e., enterprise data backups) into a single managed backup solution, which may be distributed across multiple distributed appliances.

The scope of the evaluation is defined by the Security Target [6] which identifies assumptions made during the evaluation, the intended environment for the TOE, the security functional requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2) Augmented with ALC_FLR.1. This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysia Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]).

The evaluation was performed by Securelytics Security Evaluation Facility (SEF) and the evaluation was completed on 10 August 2024.

The Malaysia Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at https://iscb.cybersecurity.my/index.php/certification/product-certification/mycc/ and the Common Criteria Recognition Arrangement at http://www.commoncriteriaportal.org

It is the responsibility of the user to ensure that Cohesity DataProtect Version 7.1.2 meets their requirements. It is recommended that a potential user of the TOE refer to the Security Target [6] and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Document Authorisation ..... **ii**

Copyright Statement ..... **iii**

Foreword ..... **iv**

Disclaimer ..... **v**

Document Change Log ..... **vi**

Executive Summary ..... **vii**

Table of Contents ..... **viii**

Index of Tables ..... **ix**

Index of Figures ..... **ix**

1 Target of Evaluation **1**

1.1 TOE Description 1

1.2 TOE Identification 2

1.3 Security Policy 3

1.4 TOE Architecture 3

1.4.1 Logical Boundaries *3*

1.4.2 Physical Boundaries *7*

1.5 Clarification of Scope 9

1.6 Assumptions 9

1.6.1 Operational Environment Assumptions *9*

1.7 Evaluated Configuration 11

1.8 Delivery Procedures 13

1.8.1 TOE Delivery *13*

1.9 Flaw Reporting Procedures 14

2 Evaluation **16**

2.1 Evaluation Analysis Activities 16

2.1.1 Life-cycle support *16*

2.1.2 Development *16*

2.1.3 Guidance documents *18*
2.1.4 IT Product Testing *18*
3 Result of the Evaluation 29
3.1 Assurance Level Information 29
3.2 Recommendation 29
Annex A References 31
A.1 References 31
A.2 Terminology 31
A.2.1 Acronyms 31
A.2.2 Glossary of Terms 32

Index of Tables

Table 1: TOE identification 2
Table 2: Cohesity DataProtect Logical Boundaries 3
Table 3: Assumptions for the TOE environment 9
Table 4: Independent Functional Test 19
Table 5: List of Acronyms 31
Table 6: Glossary of Terms 32

Index of Figures

Figure 1: Example TOE Deployment 7

1 Target of Evaluation

1.1 TOE Description

1 Cohesity DataProtect Version 7.1.2 (or collectively simply as "Cohesity"), a software suite that is used to hyperconverged secondary storage workloads (i.e., enterprise data backups) into a single managed backup solution, which may be distributed across multiple distributed appliances.

2 The intent of this product is to simplify the infrastructure and resources used to administer data backup and recovery functions across an enterprise. The TOE natively supports backups for various virtual machines, databases, and network-attached storage (NAS) devices. The TOE also interfaces natively with various cloud service providers for long-term archival and retention of backup data. Backup data stored by the TOE is protected against unauthorized modification and disclosure using symmetric encryption. The TOE provides a role-based access control policy for accessing stored data and administrative functionality.

3 Cohesity is designed to eliminate secondary storage silos by converging all secondary storage and associated data services on one unified solution – including backups, cloud gateway, files, objects, test/dev copies, and data analytics. Cohesity is a software-defined solution that spans from the edge, to the datacenter, and the cloud. With Cohesity, enterprises can:

- Simplify data protection infrastructure by converging legacy backup silos
- Consolidate file and object services
- Build a multi cloud data fabric with native cloud integration for archival, tiering and replication
- Accelerate test/dev with copy data management
- Gain visibility into their dark data with in-place analytics
- Reduce total cost of ownership for secondary storage by 50% or more

4 This capability is securely managed through user interfaces that provide granular control over authentication, authorization, and communications protocols.

5 The TSF includes the following security functions:

- Security Audit
- Cryptographic Support
- User Data Protection

- Identification and Authentication
- Security Management
- Protection of the TSF
- Resource Utilization
- Trusted Path/Channels

1.2 TOE Identification

6 The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C138
TOE Name	Cohesity DataProtect
TOE Version	Version 7.1.2
Security Target Title	Cohesity DataProtect Version 7.1.2 Security Target
Security Target Version	1.0
Security Target Date	31 July 2024
Assurance Level	Evaluation Assurance Level 2 Augmented with ALC_FLR.1
Criteria	Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [2])
Methodology	Common Methodology for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Extended CC Part 3 Conformant Package conformant to EAL 2 Augmented with ALC_FLR.1
Sponsor	Cohesity 300 Park Ave, Suite 1700, San Jose, CA 95110, USA
Developer	Cohesity 300 Park Ave, Suite 1700, San Jose, CA 95110, USA
Evaluation Facility	Securelytics SEF

	A-19-06, Tower A, Atria SOFO Suites, Jalan SS 22/23. Damansara Utama, 47400 Petaling jaya, Selangor, Malaysia

1.3 Security Policy

7 There is no organisational security policies defined regarding the use of TOE.

1.4 TOE Architecture

8 The TOE includes both physical and logical boundaries which are described in Section 2.3 & 2.4 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

9 The TOE consists of security functions provided by the TOE that are identified in the Security Target ([6]).

Table 2: Cohesity DataProtect Logical Boundaries

Security Audit	The TOE generates audits of user activity and security-relevant events that occur on the cluster, such as job failures or disk storage alerts. Audit data is distributed amongst the various nodes in the cluster to ensure that it is replicated. This stored data cannot be modified or deleted by any user or administrator. In the evaluated configuration, the various nodes are configured to send their audit data to a remote syslog server.
Cryptographic Support	The TOE supports TLS (independently and as part of HTTPS) and SSH to perform trusted communications. The TOE also uses symmetric cryptography to encrypt backup data at rest. Long-term storage of symmetric keys used to encrypt data at rest is the responsibility of the Operational Environment. Certificate data and short- term keys, such as keys established to enable TLS communications, are zeroized when no longer in use. The cryptographic functions used to secure data at rest and in transit are NIST-approved algorithm implementations.
User Data Protection	The TOE provides mechanisms for acquiring data from the operational environment for backup purposes. Data can be

	acquired from various sources such as physical servers, virtual servers, databases, storage arrays, and NAS. While the data is stored internally to the TOE, it may also be configured to be viewable as a SMB or NFS storage device. Access controls, both within the TOE's management interfaces and on any SMB/NFS shared data, are used to define the data that can be accessed by TOE and organizational users. Data at rest is protected using AES-256 encryption to prevent unauthorized access. The basic functionality for the TOE"s data protection function is to back up data from environmental sources, store it within the TOE, and use it to perform restore operations as needed. Data can be set as immutable so that an accurate reversion of working data (such as in the case of a ransomware attack) can be restored to the affected environmental systems. Policies define the data that is acquired as well as the frequency of the backup operations, as well as whether full or incremental backups are performed. Data stored on the TOE may also be sent to a remote Cloud Service Provider or a remote Cohesity Cluster (i.e. a second deployment of Cohesity) for replication or cold storage (archival) purposes. The TOE includes an Analytics Workbench application that provides a MapReduce framework for analysis and reporting on data stored within the TOE. This can be used to search for significant data, such as specific text strings/patterns, strings that may be indicative of cleartext passwords, or uncompressed video. Filters can be applied to search parameters so that, for example, data stored in a certain location or that is of a certain age can be excluded from the search. Additional custom searches can be defined by users.
Identification & Authentication	The TOE requires user authentication prior to accessing any of its security functionality. This is done using either username/password (for web GUI and SSH), public key authentication (for SSH), or token (for REST API). Multi-factor authentication (MFA) is also supported.

	Username/password data for the web GUI can be defined on the TOE or the TOE can connect to an environmental Active Directory server to perform authentication; the SSH interface uses either AD credentials or locally-defined credentials, depending on the functionality that the SSH interface is being used to perform. SSH is used to access the TOE's underlying bash shell which in turn can be used to access a support account. Integration with SSO IdPs is also supported. The TOE includes certificates signed by a Cohesity CA for its server functionality that are implicitly trusted by the TSF. These can be replaced with user-supplied certificates that are subject to validation, including revocation checking. The TSF also performs certificate validation on server certificates presented to it as part of establishing outbound trusted channels with remote servers such as Active Directory.
Security Management	The TSF provides three management interfaces: a web GUI (also known as Cohesity Dashboard), a CLI, and a REST API. The set of management functions available for use to interact with the TSF depends on the interface used to access the TOE. The TOE has five defined management roles by default. These roles grant differing degrees of access to the management functionality of the TOE. Additional roles can be defined as needed. Individual users may be restricted in the set of objects that they can perform their assigned management privileges against. In the event that management access to the TOE is lost then the host shell can be accessed through the local console. This access is only used to restore access and would not be used in normal operation.
Protection of the TSF	The TOE is deployed as a distributed system, which allows for redundant data storage. Redundancy is achieved either through the use of replication factors (i.e. duplicate copies of data stored on different disks/nodes) or erasure coding.

	The TOE performs a series of self-tests when a node is powered on. This includes validation of the cryptographic functionality, which is performed by the Cohesity OpenSSL FIPS Object Module /s`(CMVP certificate #4656). It also includes various boot checks of a node, including correct operation of OS/service boot, storage disks, and network availability. If a node experiences a failure, it will enter a degraded mode of operation and attempt to reboot. The degraded status will be reported to administrators in the management interface.
Resource Utilization	The TOE provides methods for administrators to configure replication of data across multiple nodes or Cohesity clusters. The TSF also includes a function called 'intelligent data placement' which automatically places data on appropriate nodes based on QoS and IO profiles. This ensures that access to data backup and recovery functions is maintained in the event of the failure/unavailability of individual nodes/disks or in a traffic-constrained environment.
Trusted Path/Channels	The TOE uses its FIPS-validated cryptographic module to provide secure communications between itself and remote IT entities/administrators. Specifically, the following interfaces use the following trusted channels/paths: • TOE to AD trusted channel – LDAP over TLS • TOE to remote CSP trusted channel – TLS/HTTPS • TOE to Secondary Cohesity Cluster trusted channel – TLS/HTTPS • TOE to Source trusted channel – TLS/HTTPS • TOE to Cohesity Analytics – TLS • TOE to IdP – TLS/HTTPS • Remote Source to TOE trusted channel – TLS/HTTPS

	• Remote CLI to TOE trusted path – SSH • Remote GUI to TOE trusted path – TLS/HTTPS • Remote REST API to TOE trusted path – TLS/HTTPS

1.4.2 Physical Boundaries

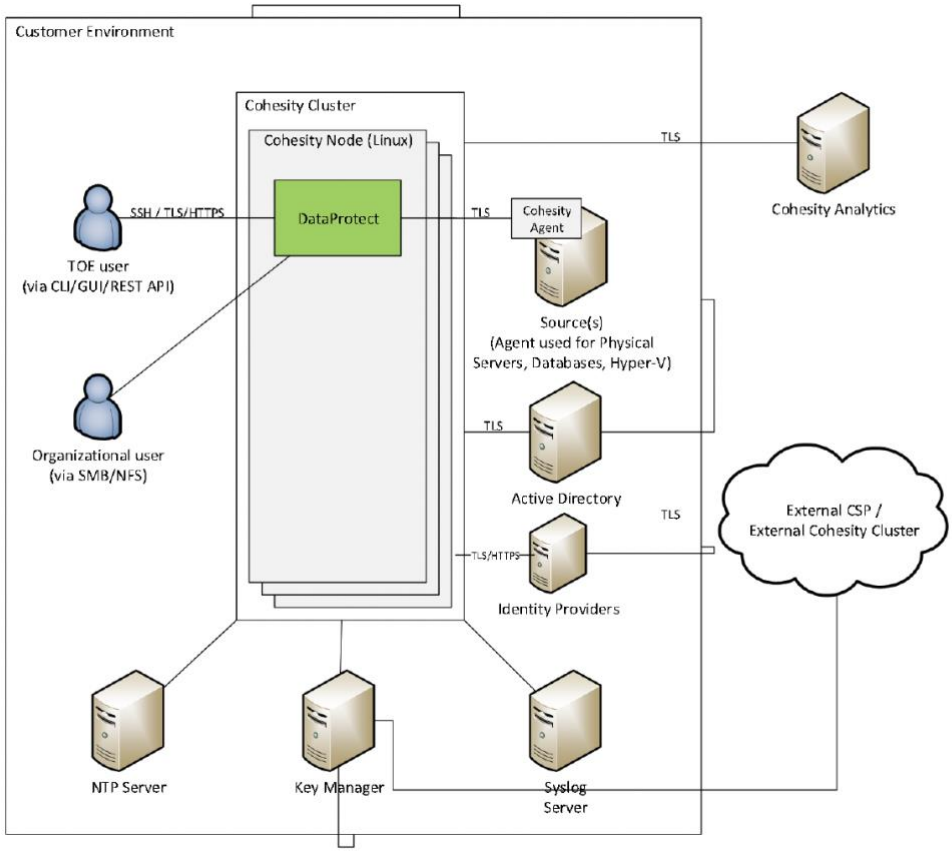

Figure 1: Example TOE Deployment

10 The components in Figure 1 are responsible for the following functions:

- TOE:
  - DataProtect: Manages confidentiality of backup data as well as backup, recovery, and archival operations:
    - Data stored on DataProtect as a View can be accessed externally via SMB/NFS
    - Other file data is only accessible through the TOE's management interfaces

11 Environmental components:

- Cohesity Node: the physical or virtual device on which the TOE software is installed
- Active Directory: user authentication
- Syslog Server: audit data storage
- NTP Server: time services
- KMIP Key Manager: data encryption key (DEK) protection
- Sources: originators of data backed up by the TOE
- Cohesity Agent: software installed on some Sources to provide an interface for the TOE to acquire the data stored on that Source
- Cloud Service Provider (CSP): offsite cold storage/replication for backup data
- External Cohesity Cluster: second deployment of Cohesity for offsite cold storage/replication of backup data
- Cohesity Analytics: Cohesity-run service for remote telemetry and support automation

12 The TOE boundary includes the DataProtect software. This software is installed on a node, which can be any of the physical and/or virtual components listed in section 2.2 above. As the TOE can be deployed as a distributed application, multiple instances of the software may be installed on multiple nodes. A combination of nodes is referred to as a cluster. A node may contain multiple individual storage disks.

13 If an instance of the TOE is deployed on a first-party hyperconverged node or supported third-party hardware, the only system requirement is that a supported hardware model is used. The dedicated hardware used for the TOE is a 2U4N system, which contains four separate nodes within one single 2U chassis, or block.

14 If an instance of the TOE is deployed on a cloud platform, the only system requirement is that Microsoft Azure, AWS, Oracle Cloud or Google Cloud is the cloud service provider (CSP) that is used.

15 If an instance of the TOE is deployed on a general-purpose computer, that computer must be running RHEL 7.9 and have a 64-bit x86 processor architecture. A representative system configuration is provided below—this configuration is identical to the C5036 hyperconverged node sold by Cohesity:

- CPU: Intel Xeon Silver 4314

- Memory: 4x32GB
- System Disk: NVMe 480GB
- Data SSD (Metadata for data backups):1.6TB
- Data HDD (for data backups): 3x12TB
- Network connectivity Options: 4x10GbE; 2x16GbE; 2x32 GbE; 2x25GbE, 4x25GbE; 2x40GbE; 2x100GbE

16 While the actual hardware on which the TOE runs is not part of the TOE, the backup data stored on this hardware is considered to be TSF data and therefore protection of it falls within the scope of the TOE.

17 Virtualized instances of the TOE can be run on VMware's ESXi/vSphere 5.1 or higher. Deploying the TOE in such a manner requires a minimum of 32GB of memory, 8 virtual CPUs and 8TB of hard disk space.

1.5 Clarification of Scope

18 The TOE is designed to be suitable for use in accordance with user guidance that is supplied with the product.

19 Section 1.4 of this document describes the scope of the evaluation, which is limited to those claims made in the Security Target (Ref [6]).

20 Potential consumers of the TOE are advised that some functions and services of the overall product have not been evaluated as part of this evaluation. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

1.6 Assumptions

21 This section summarises the security aspects of the environment/configuration in which the product is intended to operate. Consumers should understand their own IT environment and requirements for secure operation of the TOE as defined in the Security Target (Ref [6]).

1.6.1 Operational Environment Assumptions

22 Assumptions for the TOE environment as described in the Security Target (Ref [6]):

Table 3: Assumptions for the TOE environment

Assumption	Statements
A.COMPONENTS_RUNNING	It is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack or failure of one or more of the TOE components.
A.LIMITED	It is assumed that the hardware components that comprise the TOE are used only for the functionality provided by the TSF and that the TOE does not include any other general-purpose computing capabilities that present additional external interfaces to the TSF.
A.NETWORK	It is assumed that the nodes on which the TOE is deployed are connected to one another over a local network that is not subject to unauthorized surveillance.
A.PHYSICAL	It is assumed that the TOE is deployed in a location that is physically secured in its operational environment and not subject to any attacks on the physical interfaces of the TOE or the TOE hardware itself.
A.REGULAR_UPDATES	It is assumed that TOE software/firmware updates are applied on a regular schedule and/or within a reasonable period of time after they have been made available by the vendor.
A.SYSTEM_TIME	The TOE's operational environment is assumed to provide reliable system time for all nodes.
A.TRUSTED_ADMIN	It is assumed that any administrators of the TOE are trusted to be technically competent, non-malicious, and to follow operational and preparatory guidance as directed for the functions that they are authorized to perform.

1.7 Evaluated Configuration

23 The components in Figure 1 above are responsible for the following functions:

- TOE:
  - o DataProtect: Manages confidentiality of backup data as well as backup, recovery, and archival operations:
    - Data stored on DataProtect as a View can be accessed externally via SMB/NFS
    - Other file data is only accessible through the TOE's management interfaces
- Environmental components:
  - o Cohesity Node: the physical or virtual device on which the TOE software is installed
  - o Active Directory: user authentication
  - o Syslog Server: audit data storage
  - o NTP Server: time services
  - o KMIP Key Manager: data encryption key (DEK) protection
  - o Sources: originators of data backed up by the TOE
  - o Cohesity Agent: software installed on some Sources to provide an interface for the TOE to acquire the data stored on that Source
  - o Cloud Service Provider (CSP): offsite cold storage/replication for backup data
  - o External Cohesity Cluster: second deployment of Cohesity for offsite cold storage/replication of backup data
  - o Cohesity Analytics: Cohesity-run service for remote telemetry and support automation

24 The TOE requires the following components in its operational environment to support the enforcement of its security functions:

- Cohesity Node: the physical or virtual device on which the TOE software is installed
- Physical/logical storage capable of having backup data ingested by the TSF (also known as Sources) – any of the following are supported:
  - o Virtual servers: VMware, Hyper-V, AHV, RHV
  - o Physical servers: Windows, Linux, IBM AIX, Solaris, HP-UX

o Applications: Microsoft Exchange

o Databases: Microsoft SQL Server, Oracle, SAP, CockroachDB, IBM DB 2, PostgreSQL

o Storage integrations: Pure Storage FlashArray, Cisco HyperFlex, Nimble Storage, HPE Alletra, NetApp ONTAP, Nutanix

o Network Attached Storage: NetApp ONTAP cluster, Dell EMC Isilon, Pure Storage FlashBlade, Elastifile EFS, IBM GPFS, NFSv3, NFSv4.1, SMB 2.0, SMB 3.0

o QStarTape

o NoSQL

o Hadoop

● Cohesity Agent: installed on the following Sources to provide an interface to transfer data from that Source to the TOE:

o Virtual servers: Hyper-V (or SCVMM server containing multiple Hyper-V VMs), VMware, AHV, RHV

o Physical Servers: all

o Databases: all

o SQL Servers

o Exchange Servers

● Web browser with HTML5 support (for administration). Any browser that supports TLS 1.2/1.3 and HTML5 is acceptable.

● SSH client (for administration). Any client that uses SSH 2.0 is acceptable.

● KMIP-compliant Key Manager (for management and secure storage of DEKs)

25 The TOE may or may not make use of the following environmental components, depending on how it is configured:

● VMware vSphere (6.7 or higher) or Microsoft Hyper-V server (2016, 2019 or 2022): required if Cohesity Virtual Edition is used

● Active Directory: optional for authentication and authorization

● DNS Server: optional for use of name services

● NTP Server: optional for use of network time

● Syslog Server: optional for remote storage of audit data

● CSP (Microsoft Azure, AWS, Google Cloud, Oracle, or any S3 compatible private cloud or on-premises object storage): optional for use of cloud backup

● External Cohesity Cluster: optional for replication of stored data

● Cohesity Analytics: optional service run by Cohesity for remote telemetry and support automation.

1.8 Delivery Procedures

26 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

27 The delivery procedures should consider, if applicable, issues such as:

- ensuring that the TOE received by the consumer corresponds precisely to the evaluated version of the TOE;
- avoiding or detecting any tampering with the actual version of the TOE;
- preventing submission of a false version of the TOE;
- avoiding unwanted knowledge of distribution of the TOE to the consumer: there might be cases where potential attackers should not know when and how it is delivered;
- avoiding or detecting the TOE being intercepted during delivery; and
- avoiding the TOE being delayed or stopped during distribution.

1.8.1 TOE Delivery

1.8.1.1 Software Delivery

28 TOE software is securely delivered from the Cohesity Support Portal protected by username/password. The software package integrity is verified using digital signature (ECDSA 384 + SHA-512) during upgrade package installation. Download portal also publishes the SHA-256 and MD5 hashes of the binaries for binary integrity verification. When there is a new release of software, email notification is sent to the customer and also the online portal is updated with the new information (link and version). All the manuals associated with the software are also linked to the online portal.

1.8.1.2 Software Delivery

29 The TOE is a software application that can be scaled across physically distributed nodes. Customer orders the hardware components via a reseller/distributor who ships

the order. Since Cohesity is not selling the hardware, shipments are delivered via the reseller/distributor's carrier of choice to the end customer directly.

30 Once an order is received, ship notification is sent via email. A packing slip on box with model number and serial number matching the packing slip to hardware is sent to the customer. Product name on physical packaging and physical chassis includes top level hardware extended SKU configuration, i.e. C5016-10G-SFP-4 on a bar-coded label and model number on the compliance tick label. Interactive setup/installation materials include high level SKU depending on platform and NIC configuration. There are multiple options - "C5000 Series" for SFP, RJ45 and FC HBAs.

31 Hardware components include security tape. Palletized Cartons are sealed with kraft sealing tape, polyester straps and tamper evident security tape. Cartons have the Cohesity logo in black on each side.

1.9 Flaw Reporting Procedures

32 The evaluator examined the flaw remediation procedures documentation and determined that it describes the procedures used to track all reported security flaws in each release of the TOE which would produce a description of each security flaw in terms of its nature and effects.

33 The evaluator examined the flaw remediation procedures and determined that the application of the procedures would identify the status of finding a correction to each security flaw and identify the corrective action for each security flaw.

34 The evaluator examined the flaw remediation procedures documentation and determined that it describes a means of providing the TOE users with the necessary information on each security flaw.

35 The evaluator examined the flaw remediation procedures and determined that it describes procedures for the developer to accept reports of security flaws or requests for corrections to such flaws.

36 The evaluator examined the flaw remediation procedures and determined that the application of the procedures would help to ensure reported flaw is corrected and that TOE users are issued remediation procedures for each security flaw.

37 The evaluators examined the flaw remediation procedures and determined that the application of the procedures would result in safeguards that the potential correction contains no adverse effects.

38 The evaluators examined the flaw remediation guidance and determined that the application of the procedures would result in a means for the TOE user to provide reports of suspected security flaws or requests for corrections to such flaws.

39 Therefore, the evaluator confirms that the information provided meets all requirements for content and presentation of evidence.

2 Evaluation

41 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 5 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 5 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2 Augmented with ALC_FLR.1. The evaluation was performed conformant to the MyCC Scheme Requirement (MyCC_REQ) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

2.1 Evaluation Analysis Activities

42 The evaluation activities involved a structured evaluation of the TOE, including the following components:

2.1.1 Life-cycle support

43 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the configuration items were clearly and uniquely labelled, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorised access to the configuration items. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.

44 The evaluators confirmed that the configuration list includes TOE itself, the parts that comprise the TOE the evaluation evidence required by the SARs in the the Security Target (Ref [6]).

45 The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

2.1.2 Development

Architecture

46 The evaluators examined the security architecture description (contained in Section 4) and determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

47 The security architecture description describes the security domains maintained by the TSF.

48 The initialisation process described in the security architecture description preserves security.

49 The evaluators examined the security architecture description and concluded that it contains sufficient information to demonstrate that the TSF is able to protect itself from tampering by untrusted active entities. The security architecture description presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

Functional Specification

50 The evaluators examined the functional specification and determined that:

- The TSF is fully represented;
- It states the purpose of each TSF Interface (TSFI); and
- The method of use for each TSFI is given.

51 The evaluators also examined the presentation of the TSFI and determined that:

- It completely identifies all parameters associated with every TSFI; and
- It completely and accurately describes all error messages resulting from an invocation of each SFR-enforcing TSFI.

52 The evaluators also confirmed that the developer supplied tracing links of the SFRs to the corresponding TSFIs.

TOE Design Specification

53 The evaluators examined the TOE design (contained in [8]) and determined that the structure of the entire TOE is described in terms of subsystems.

54 The evaluators also determined that all subsystems of the TSF are identified.

55 The evaluators determined that interactions between the subsystems of the TSF were described.

56 The evaluators found the TOE design to be a complete, accurate, and detailed description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

57 The evaluators examined the TOE design and determined that it provides a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

58 The evaluators determined that the TOE design contained a complete and accurate mapping from the TSFI described in the functional specification to the subsystems of the TSF described in the TOE design.

59 The evaluators determined that all SFRs were covered by the TOE design and concluded that the TOE design was an accurate instantiation of all SFRs.

2.1.3 Guidance documents

60 The evaluators examined the operational user guidance determined that it describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings. For each role, the secure use of available TOE interfaces is described. The available security functionality and interfaces are described for each user role – in each case, all security parameters under the control of the user are described with indications of secure values where appropriate.

61 The operational user guidance describes, for each user role, each type of security-relevant event relative to the user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.

62 The evaluators examined the operational user guidance in conjunction with other evaluation evidence and determined that the guidance identifies all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

63 The evaluators determined that the operational user guidance describes, for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

64 The evaluators confirmed that the TOE guidance fulfilled all the requirements and passed for this class.

2.1.4 IT Product Testing

65 Testing at EAL 2 Augmented with ALC_FLR.1 consists of assessing developer tests, performing independent functional test, and conducting penetration tests. The TOE testing was conducted by Securelytics SEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Report.

2.1.4.1 Assessment of Developer Tests

66 The evaluators verified that the developer has met their testing responsibilities by repeating some developer test, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator). The results of the evaluators' tests are consistent with the developers' test results defined in their evaluation evidences submitted.

2.1.4.2 Independent Functional Testing

67 At EAL 2 Augmented with ALC_FLR.1, independent functional testing is the evaluation conducted by evaluators based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing a subset of the developer's test plan, and creating test cases that are independent of the developer's tests.

68 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests were recorded by the evaluators and are consistent with the expected test results in the test documentation.

Table 4: Independent Functional Test

TEST ID	DESCRIPTIONS	RESULTS
F001 – Identification and Authentication FIA_UAU.2 FIA_UID.2	• To verify that the TOE require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user • To verify that the TOE require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user	Passed. Result as expected.
F002 – Security Management and User Data Protection FMT_MOF.1	• To verify that the TOE restricts the ability to disable, enable, modify the behavior of, execute the functions audit, backup, restore, archival, DataLock, storage redundancy, clone, analytics to roles defined in FMT_SMR.2 according to the specified rules for each roles.	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
FMT_MTD.1 FMT_SMF.1 FMT_SMR.2 FDP_ACC.1 FDP_ACF.1 FDP_ETC.1 FDP_IMM_EXT.1 FDP_ITC.1 FDP_SAR_EXT.1 FDP_SDC_EXT.1	• To verify that the TOE restricts the ability to query, modify, delete, create the cluster configuration, external target, policy, storage domain, backup, View, Source, snapshot, user, role data to roles defined in FMT_SMR.2 according to the specified rules. • To verify that the TOE can perform the management functions: Access Management, Clone Management, Cluster Management, Data Protection, Recovery Management, Storage Management, Analytics Management, and Source Access Control. • To verify that the TOE maintains the roles: Admin, Operator, Viewer, Self Service Data Protection, Data Security, and administrator-defined roles. • To verify that the TOE can associate users with roles such as Admin, Operator, Viewer, Self Service Data Protection, Data Security, and administrator-defined roles. • To verify that the TOE ensures that no multiple roles for administrative users, no role for organizational user are satisfied. • To verify that the TSF enforces the data access control policy based on TOE users, organizational users via SMB, and organizational users via NGS according to the specified rules. • To verify that the TSF enforces the rules determining allowed operations among controlled subjects and objects for roles such as Admin, Operator, Self Service Data Protection,	

TEST ID	DESCRIPTIONS	RESULTS
	Data Security, Viewer, and administrator-defined roles. • To verify that the TSF explicitly authorize access of subjects to objects based on the specified additional rules for roles like Admin, Operator, Viewer, and Self Service Data Protection. • To verify that the TSF explicitly denies access of subjects to objects based on the specified additional rules, ensuring roles such as Viewer and organizational users cannot modify or delete Views with the DataLock property set. • To verify that the TSF enforces the data access control policy when exporting user data to a remote CSP or Cohesity Cluster outside of the TOE, ensuring user data is exported without associated security attributes, and this applies to all roles. • To verify that the TSF prevents the modification of stored user data by using read-only Snapshots and DataLock attribute, appliance to all roles. • To verify that the TSF enforces the data access control policy when importing user data from outside the TOE, ignoring any associated security attributes, for all roles. • To verify that the TSF provides TOE users with the Reporting privilege the capability to read specified data types from Snapshots or files stored directly on a View. • To verify that the TSF provides the ability to apply filtering based on user-specified inputs for search data.	

TEST ID	DESCRIPTIONS	RESULTS
	• To verify that the TSF ensures the confidentiality of stored user data by using AES encryption with unique encryption keys per Storage Domain, applicable to all roles.	
F003 – Security Audit FAU_GEN.1 FAU_GEN.2 FAU_STG.1	• To verify that the TOE able to generate an audit record of the following auditable events: a. Start-up and shutdown of the audit functions; b. All auditable events for the level of audit; c. Additional cluster audit events in Table 2 of ST (SMB/NFS file audit events for the following operations such as mount, create, delete, rename, set attributes. • To verify that the TOE record within each audit record at least the following information: a. Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and b. For each audit event type, based on the auditable event definitions of the functional components; c. For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event. • To verify that the TOE protect the stored audit records in the audit trail from unauthorized deletion. • To verify that the TOE able to prevent unauthorized modifications to the stored audit records in the audit trail	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
F004 – Cryptographic Support (FCS) FCS_CKM.1 FCS_CKM.4 FCS_COP.1(1) FCS_COP.1(2) FCS_COP.1(3) FCS_COP.1(4) FCS_HTTPS_EXT.1 FCS_RBG_EXT.1 FCS_SSH_EXT.1 FCS_TLS_EXT.1	• To verify that the TOE generates cryptographic keys using elliptic curve cryptography with the NIST P-384 curve and 384-bit key size, compliant with FIPS 186-4. • To verify that the TOE destroys cryptographic keys using the key zeroization method, compliant with FIPS 140-2. • To verify that the TOE performs symmetric encryption and decryption using AES in CBC, GCM, and CTR modes with key sizes of 128, 192, and 256 bits, compliant with NIST SP 800-38. • To verify that the TOE performs digital signature generation and verification using RSA with 2048-bit keys and ECDSA with 256-bit keys, compliant with FIPS 186-2 (RSA) and FIPS 186-4 (ECDSA). • To verify that the TOE performs cryptographic hashing using SHA-1 and SHA-2 with key sizes of 160, 256, 384, and 512 bits, compliant with FIPS 180-4. • To verify that the TOE performs keyed-hash message authentication using HMAC with key sizes equal to block sizes of 160, 256, 384, and 512 bits, compliant with FIPS 198-1. • To verify that the TOE implements the HTTPS protocol compliant with RFC 2818. • To verify that the TOE implements the HTTPS protocol using TLS. • To verify that the TOE performs deterministic random bit generation services using CTR_DRBG (AES), compliant with ISO/IEC	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
	18031:2011, and is seeded by at least one software-based noise source with a minimum of 256 bits of entropy. • To verify that the TOE implements the SSH protocol compliant with RFCs 4251, 4252, 4253, 4254, 5647, 5656, and 6668. • To verify that the TOE ensures the SSH protocol implementation supports public key-based and password-based authentication methods • To verify that packets greater than 65535 bytes in an SSH transport connection are dropped. • To verify that the TOE ensures the SSH transport implementation uses only the following encryption algorithms: aes128-gcm@openssh.com, aes256-gcm@openssh.com, aes128-ctr, aes192-ctr, and aes256-ctr. • To verify that the TOE ensures the SSH public-key based authentication implementation uses only ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, and the specified certificate algorithms. • To verify that the TOE ensures the SSH transport implementation uses only hmac-sha2-256 and hmac-sha2-512 as its MAC algorithms and rejects all others. • To verify that the TOE ensures ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, and diffie-hellman-group-exchangesha256 are the only allowed key exchange methods for the SSH protocol.	

TEST ID	DESCRIPTIONS	RESULTS
	• To verify that the TOE implements TLS versions 1.2 and 1.3 and rejects all other TLS and SSL versions. • To verify that the TOE supports the following TLS ciphersuites: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_CHACHA20_POLY1305_SHA256, TLS_AES_256_GCM_SHA384, and TLS_AES_128_GCM_SHA256.	
F005 – Protection of TSF and Resource Utilization FPT_FLS.1 FPT_TST_EXT.1 FRU_FLT.1	• To verify that the TOE preserve a secure state when node failure, HDD failure, SSD failure, power supply failure, self-test failures occur. • To verify that the TOE run a suite of the following self-tests *during initial start-up on power on* to demonstrate the correct operation of the TSF such as services and dependencies self-test, file system integrity self-test, node availability self-test and cryptographic self-tests. • To verify that the TOE ensure the operation of data availability when the disk or node failure, power supply failure failures occur	Passed. Result as expected.
F006 – Trusted Path/Channel FTP_ITC.1 FTP_TRP.1	• To verify that the TOE provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
	• To verify that the TOE permit the TSF, another trusted IT product to initiate communication via the trusted channel. • To verify that the TOE initiate communication via the trusted channel for backup, recovery, replication, and archival of backup data, remote audit data storage, Active Directory user authentication, Cohesity Analytics, Identity Provider for SSO. • To verify that the TOE provide a communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification, disclosure. • To verify that the TOE permit remote users to initiate communication via the trusted path. • To verify that the TOE require the use of the trusted path for initial user authentication, all subsequent user interactions.	

99 All testing performed by evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.3 Penetration testing

100 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, functional specification, TOE design, and security architecture description.

101 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attack performed by an attacker possessing a basic attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapsed time);

b) Specialist technical expertise required (specialised expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

e) IT hardware/software or other requirement for exploitation

102 The evaluators' search for vulnerabilities also considered public domain sources for published vulnerability data related to the TOE and the contents of all TOE deliverables. The following public domain sources were searched:

a) www.google.com

b) www.yahoo.com

c) www.bing.com

d) www.cve.mitre.org

103 The penetration tests focused on:

a) SQL Injection;

b) Server-Side template Injection;

c) Cross site scripting;

d) Failure to restrict URL Access;

e) Directory Traversal;

f) Sensitive Data Exposure – Browser;

g) Error messages;

h) Sensitive Data Exposure – Server;

i) Sensitive Information in Cookie;

j) User Account Lockout;

k) Security Misconfiguration – Cookies;

l) SSL Configuration;

m) TOE Connectivity Check;

n) Traceroute IP;

o) Banner Grabbing;

p) Firewalk Scanning;

q) Denial of Service;

r) TCP SYN flood attack;

s) ICMP Smurf Attack;

t) SSH port brute force attack;

u) Search of vulnerability in public vulnerabilities repositories; and

v) Information leakage via unencrypted network traffic.

104 The result of the penetration testing noted that there is no residual vulnerability found. However, it is important to ensure that the TOE is used only in its evaluated configuration and in a secure environment as specified in Section 4 of the Security Target (Ref [6].

2.1.4.4 Testing Results

105 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and its functional specification. Therefore, the certifiers confirmed that all tests conducted were PASSED as expected.

3 Result of the Evaluation

106 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7], the Malaysian Common Criteria Certification Body certifies the evaluation of Cohesity DataProtect Version 7.1.2 performed by Securelytics SEF.

107 Securelytics SEF found that Cohesity DataProtect Version 7.1.2 upholds the claims made in the Security Target (Ref [6] and supporting documentations and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 2 Augmented with ALC_FLR.1.

108 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. The risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

109 EAL 2 Augmented with ALC_FLR.1 provides assurance by a full security target and analysis of the SFRs in that Security Target, using functional and complete interface specifications, guidance documentation and a description of the design of the TOE to understand the security behaviours.

110 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

111 EAL 2 Augmented with ALC_FLR.1 also provides assurance through use of a configuration management system, the secure delivery procedures, and evidence of flaw remediation procedures.

3.2 Recommendation

112 The Malaysian Certification Body (MyCB) is strongly recommends that:

a) The users should make themselves familiar with the developer guidance provided with the TOE, and to pay attention to all security warnings as well as to observe the

operational environment requirements and assumptions defined in the applicable Security Target (Ref [6].

b) The users must maintain the confidentiality, integrity and availability of security relevant data for TOE initialization, start-up and operation if stored or handled outside the TOE.

c) The System Administrator should review the audit trail generated and exported by the TOE periodically.

d) The users must ensure appropriate network protection is maintained, the network on which the TOE is installed must be both physically and logically protected.

Annex A References

A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July, 2014.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[3] The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[4] MyCC Scheme Requirement (MYCC_REQ), v1b, CyberSecurity Malaysia, July 2023.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v3, January 2023.

[6] Cohesity DataProtect Version 7.1.2 Security Target, Version 1.8, 31 July 2024.

[7] Cohesity DataProtect Version 7.1.2, Evaluation Technical Report, Version 1.0, 19 August 2024.

[8] Cohesity DataProtect Version 7.1.2 Design Documentation, Version 1.0, 31 July 2024.

A.2 Terminology

A.2.1 Acronyms

Table 5: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile

Acronym	Expanded Term
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 6: Glossary of Terms

Term	Definition and Source
CC International Interpretation	An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC 17065
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.

Term	Definition and Source
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.

--- END OF DOCUMENT ---