Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 7/22

(Certification No.)

Prodotto: Distributed Services Platform v1.28.0-E-96

(Product)

Sviluppato da: Pensando Systems, Inc.

(Developed by)

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL2+
(ALC_FLR.2)

Il Direttore
(Dott.ssa Eva Spina)

Firmato digitalmente da Eva Spina
Data: 2022.03.11 09:26:44 +01'00'

Roma, 11 marzo 2022

Common Criteria

SOGIS IT SECURITY CERTIFIED

Questa pagina è lasciata intenzionalmente vuota

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Rapporto di Certificazione

Distributed Services Platform v1.28.0-E-96

OCSI/CERT/CCL/09/2020/RC

Versione 1.0

11 marzo 2022

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	11/03/2022

2 Indice

3 Elenco degli acronimi

AD	Active Directory
API	Application Programming Interface
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
DPCM	Decreto del Presidente del Consiglio dei Ministri
DSC	Distributed Services Card
DSP	Distributed Services Platform
EAL	Evaluation Assurance Level
IPFIX	Internet Protocol Flow Information Export
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
MAC	Media Access Control
NIS	Nota Informativa dello Schema
NTP	Network Time Protocol
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
OS	Operating System
PP	Protection Profile
PSM	Policy and Services Manager
RADIUS	Remote Authentication Dial-In User Service
REST	Representational State Transfer
RFV	Rapporto Finale di Valutazione

SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Arrangement
ST	Security Target
TDS	Traguardo di Sicurezza
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
UI	User Interface
VM	Virtual Machine

4 Riferimenti

4.1 Criteri e normative

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[SOGIS] “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, Version 3, January 2010

4.2 Documenti tecnici

[DSC25] “Pensando Distributed Services Card DSC-25 User Guide for Enterprise Edition”, Version 3.0, Pensando Systems, Inc., August 2021

[DSC100] “Pensando Distributed Services Card DSC-100 User Guide for Enterprise Edition”, Version 2.0, Pensando Systems, Inc., August 2021

[DSPDBP] “Pensando Policy and Services Manager, Enterprise Edition Design Best Practice Guide”, Version 1.7, Pensando Systems, Inc., August 2021

[DSPGDS] “Pensando Systems, Inc. Distributed Services Platform v1.28.0-E-96 Guidance Documentation Supplement”, Version 0.4, Corsec Security, Inc., 26 January 2022.

[DSPLDAP] “Pensando Policy and Services Manager, LDAP Server Configuration Guide”, Version 1.5, Pensando Systems, Inc., September 2020

[DSPRN] “Pensando Distributed Services Platform, Enterprise Edition Release Notes Version 1.28.0-E”, Version 3.1, Pensando Systems, Inc., August 2021

[DSPTG] “Pensando Distributed Services Platform, Enterprise Edition Troubleshooting Guide”, Version 2.0, Pensando Systems, Inc., August 2021

[DSPUG] “Pensando Policy and Services Manager, Enterprise Edition User Guide”, Version 2.0, Pensando Systems, Inc., July 2021

[RFV] “Pensando Distributed Services Platform v1.28.0-E-96” Evaluation Technical Report, v1, CCLab Software Laboratory, 25 February 2022

[TDS] “Pensando Systems, Inc. Distributed Services Platform v1.28.0-E-96 Security Target”, Version 0.6, Corsec Security, Inc., 26 January 2022

5 Riconoscimento del certificato

5.1 Riconoscimento di certificati CC in ambito europeo (SOGIS-MRA)

L'accordo di mutuo riconoscimento in ambito europeo (SOGIS-MRA, versione 3, [SOGIS]) è entrato in vigore nel mese di aprile 2010 e prevede il riconoscimento reciproco dei certificati rilasciati in base ai Common Criteria (CC) per livelli di valutazione fino a EAL4 incluso per tutti i prodotti IT. Per i soli prodotti relativi a specifici domini tecnici è previsto il riconoscimento anche per livelli di valutazione superiori a EAL4.

L'elenco aggiornato delle nazioni firmatarie e dei domini tecnici per i quali si applica il riconoscimento più elevato e altri dettagli sono disponibili su https://www.sogis.eu/.

Il logo SOGIS-MRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito SOGIS-MRA per tutti i componenti di garanzia dichiarati.

5.2 Riconoscimento di certificati CC in ambito internazionale (CCRA)

La versione corrente dell'accordo internazionale di mutuo riconoscimento dei certificati rilasciati in base ai CC (Common Criteria Recognition Arrangement, [CCRA]) è stata ratificata l'8 settembre 2014. Si applica ai certificati CC conformi ai Profili di Protezione "collaborativi" (cPP), previsti fino al livello EAL4, o ai certificati basati su componenti di garanzia fino al livello EAL2, con l'eventuale aggiunta della famiglia Flaw Remediation (ALC_FLR).

L'elenco aggiornato delle nazioni firmatarie e dei Profili di Protezione "collaborativi" (cPP) e altri dettagli sono disponibili su https://www.commoncriteriaportal.org/.

Il logo CCRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito CCRA per tutti i componenti di garanzia dichiarati.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "Distributed Services Platform v1.28.0-E-96", nel seguito del documento anche indicato come "DSP", sviluppato da Pensando Systems, Inc.

L'ODV è una combinazione di software e firmware che fornisce servizi di rete a livello di interfaccia per i server in un data center aziendale. La piattaforma è composta da schede chiamate Distributed Services Cards (DSC) installate su ciascun server e da un cluster di Policy and Services Manager (PSM) che gestisce le schede DSC da un punto centralizzato all'interno del data center.

La valutazione è stata condotta in accordo ai requisiti stabiliti dallo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione ed espressi nelle Linee Guida Provvisorie [LGP1, LGP2, LGP3] e nelle Note Informative dello Schema [NIS1, NIS2, NIS3]. Lo Schema è gestito dall'Organismo di Certificazione della Sicurezza Informatica, istituito con il DPCM del 30 ottobre 2003 (G.U. n.98 del 27 aprile 2004).

Obiettivo della valutazione è fornire garanzia sull'efficacia dell'ODV nel rispettare quanto dichiarato nel Traguardo di Sicurezza [TDS], la cui lettura è consigliata ai potenziali acquirenti e/o utilizzatori. Le attività relative al processo di valutazione sono state eseguite in accordo alla Parte 3 dei Common Criteria [CC3] e alla Common Evaluation Methodology [CEM].

- L'ODV è risultato conforme ai requisiti della Parte 3 dei CC v 3.1 per il livello di garanzia EAL2, con l'aggiunta di ALC_FLR.2, in conformità a quanto riportato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in Pensando Distributed Services Platform, Enterprise Edition Release Notes Version 1.28.0-E [DSPRN]

- Pensando Policy and Services Manager, Enterprise Edition User Guide [DSPUG]

- Pensando Policy and Services Manager LDAP Server Configuration Guide [DSPLDAP]

- Pensando Distributed Services Platform, Enterprise Edition Troubleshooting Guide [DSPTG]

- Pensando Policy and Services Manager, Enterprise Edition Design Best Practice Guide [DSPDBP]

- Pensando Distributed Services Card DSC-25 User Guide for Enterprise Edition [DSC25]

- Pensando Distributed Services Card DSC-100 User Guide for Enterprise Edition [DSC100]

- Pensando DSP Guidance Documentation Supplement [DSPGDS]

Appendice B – Configurazione valutata di questo Rapporto di Certificazione.

La pubblicazione del Rapporto di Certificazione è la conferma che il processo di valutazione è stato condotto in modo conforme a quanto richiesto dai criteri di valutazione Common Criteria – ISO/IEC 15408 ([CC1], [CC2], [CC3]) e dalle procedure indicate dal Common Criteria Recognition Arrangement [CCRA] e che nessuna vulnerabilità sfruttabile è stata trovata. Tuttavia l'Organismo di Certificazione con tale documento non esprime alcun tipo di sostegno o promozione dell'ODV.

7 Riepilogo della valutazione

7.1 Introduzione

Questo Rapporto di Certificazione specifica l'esito della valutazione di sicurezza del prodotto "Distributed Services Platform v1.28.0-E-96" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti e/o utilizzatori per giudicare l'idoneità delle caratteristiche di sicurezza dell'ODV rispetto ai propri requisiti.

Il presente Rapporto di Certificazione deve essere consultato congiuntamente al Traguardo di Sicurezza [TDS], che specifica i requisiti funzionali e di garanzia e l'ambiente di utilizzo previsto.

7.2 Identificazione sintetica della certificazione

Nome dell'ODV	Distributed Services Platform v1.28.0-E-96
Traguardo di Sicurezza	"Pensando Systems, Inc. Distributed Services Platform v1.28.0-E-96 Security Target", Version 0.6 [TDS]
Livello di garanzia	EAL2 con l'aggiunta di ALC_FLR.2
Fornitore	Pensando Systems, Inc.
Committente	Corsec Security, Inc.
LVS	CCLab Software Laboratory
Versione dei CC	3.1 Rev. 5
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	1° dicembre 2020
Data di fine della valutazione	25 febbraio 2022

I risultati della certificazione si applicano unicamente alla versione del prodotto indicata nel presente Rapporto di Certificazione e a condizione che siano rispettate le ipotesi sull'ambiente descritte nel Traguardo di Sicurezza [TDS].

7.3 Prodotto valutato

In questo paragrafo vengono sintetizzate le principali caratteristiche funzionali e di sicurezza dell'ODV; per una descrizione dettagliata, si rimanda al Traguardo di Sicurezza [TDS].

L'ODV "Distributed Services Platform v1.28.0-E-96" è una combinazione di software e firmware che fornisce servizi di rete a livello di interfaccia per i server in un data center aziendale. L'ODV è composto da tre istanze del software di un nodo del Policy and Services Manager (PSM) e più istanze del firmware di una scheda DSC (Distributed Services Card). Il software dei nodi PSM e il firmware delle DSC vengono eseguiti

rispettivamente su macchine virtuali (VM) e hardware DSC presenti nell'ambiente operativo. Entrambi i gruppi di questi componenti vengono eseguiti su *host* server separati.

L'ODV ha la capacità di generare record di audit per eventi relativi alla gestione di criteri di avviso, destinazioni di avviso, account di utente dell'ODV, metodi di autenticazione, ruoli, sessioni di *mirroring* e *host* DSC. L'ODV può anche generare record di audit per attività non gestionali, inclusi autenticazione, modifiche delle password e errori dei nodi. Tutti i record di audit contengono l'identità dell'utente dell'ODV che ha eseguito l'operazione che ha causato un audit, se applicabile. Sulla base degli eventi di audit generati, l'ODV permette di impostare regole per il monitoraggio di criteri definiti dall'amministratore, sulla base dei quali inviare avvisi al server *syslog* nell'ambiente operativo. Questi avvisi possono essere utilizzati per notificare agli utenti dell'ODV potenziali violazioni della sicurezza. L'ODV fornisce anche due aree per l'analisi degli eventi di audit generati dall'ODV, che sono limitate agli utenti dell'ODV con il ruolo di AdminRole o con il permesso All. L'ODV utilizza la fonte temporale dell'*host* per fornire marcature temporali affidabili per gli eventi di audit.

L'ODV fornisce all'interno delle sue interfacce diverse aree di gestione, che includono criteri di avviso, destinazioni di avviso, account, ruoli, metodi di autenticazione, *host* DSC e sessioni di *mirroring*. L'ODV gestisce il ruolo predefinito AdminRole e può gestire un numero qualsiasi di ruoli definiti dall'amministratore. L'ODV è anche in grado di preservare il proprio stato sicuro e rimanere pienamente funzionante in caso di guasto di un nodo PSM.

Per una descrizione dettagliata dell'ODV, si consulti il par. 1.3 e il par. 1.4 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito.

7.3.1 Architettura dell'ODV

L'ODV è costituito da diverse copie del firmware DSC e da un cluster di tre nodi del software PSM. Lo stesso firmware DSC viene eseguito su più schede DSC che differiscono per tipo di interfaccia e fattore di forma, ma possono essere installate in qualsiasi server di un data center. Le schede vengono gestite dal cluster PSM tramite il firmware DSC.

In Figura 1 sono illustrati l'ambito e il confine fisico dell'ODV.

Il cluster PSM consente la configurazione e l'inoltro dei dati di rete e delle politiche di osservabilità alle schede Pensando DSC da una posizione centralizzata. Ogni nodo nel cluster PSM viene eseguito su una macchina virtuale. Durante la configurazione iniziale viene assegnato un nodo leader e i vari nodi lavorano in quorum quando prendono decisioni. L'architettura dei nodi è costituita da contenitori Docker e microservizi realizzati da controllori Kubernetes. Un cluster PSM può gestire migliaia di DSC e il relativo firmware.

Il firmware DSC è installato su un chip Pensando Capri disponibile sulle schede Pensando DSC-25 e Pensando DSC-100. Il firmware DSC fornisce dati di telemetria e analisi, *mirroring* ed esportazioni IPFIX dal server su cui sono installati per consentire agli amministratori di data center di visualizzare e comprendere il traffico di rete su ciascun server. Il firmware DSC comunica con il cluster PSM attraverso un canale TLS con autenticazione reciproca.

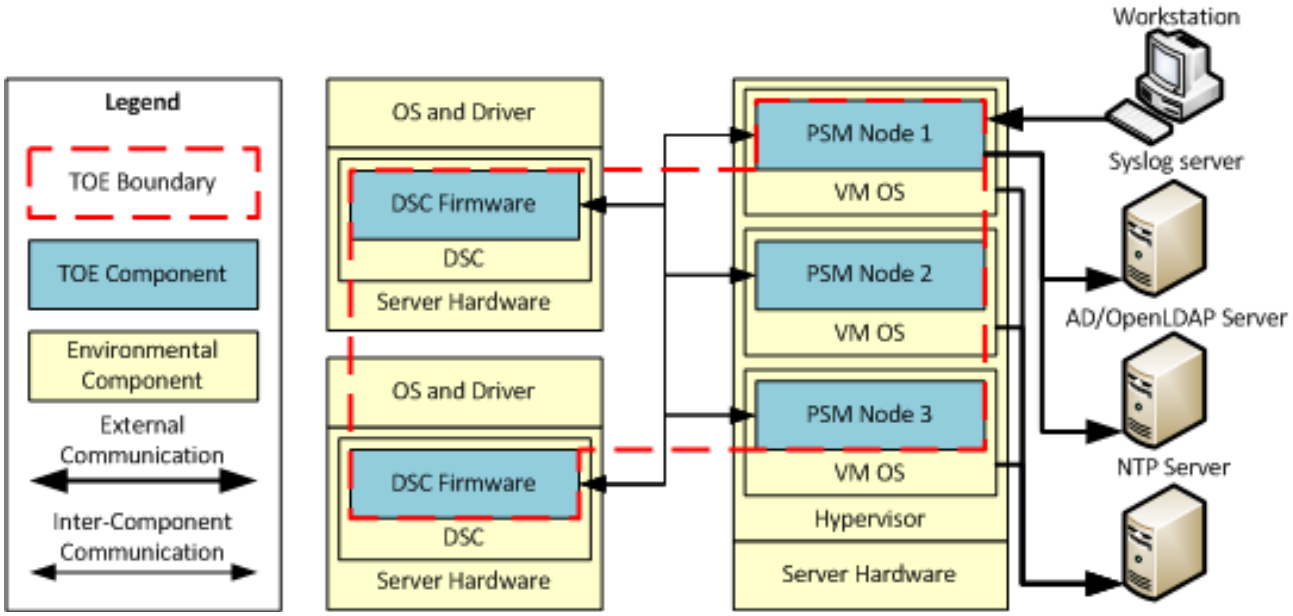

Figura 1 - Confine fisico dell'ODV

7.3.2 Caratteristiche di sicurezza dell'ODV

Il problema di sicurezza dell'ODV, comprendente obiettivi di sicurezza, ipotesi, minacce e politiche di sicurezza dell'organizzazione, è definito nel cap. 3 del Traguardo di Sicurezza [TDS].

Per una descrizione dettagliata delle Funzioni di Sicurezza dell'ODV, si consulti il cap. 7 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito:

- **Audit di sicurezza**: l'ODV genera record di audit per eventi relativi all'avvio e all'arresto della funzione di audit, all'autenticazione, alle modifiche delle password, agli errori dei nodi e alle operazioni di gestione. L'ODV è in grado di associare i record di audit all'utente dell'ODV che ha causato l'evento. I record di audit sono presentati in modo leggibile e sono visualizzabili solo dagli utenti al cui account è assegnato il ruolo AdminRole o un ruolo con assegnato il permesso All.
  L'ODV controlla altresì gli eventi di audit generati sulla base di criteri definiti dall'amministratore e, in caso tali criteri siano soddisfatti, invia un avviso a un server *syslog*.

- **Identificazione e autenticazione**: per ciascun account locale l'ODV mantiene i seguenti attributi di sicurezza: nome completo, Email, ruoli, identificativo di login, password e tipo di autenticazione. L'ODV garantisce che quando viene impostata una password vengano applicate le regole di complessità prestabilite. L'ODV maschera i caratteri delle password durante l'inserimento utilizzando il carattere "•" (pallino pieno).
  L'ODV richiede che l'utente sia identificato e autenticato prima di poter intraprendere qualsiasi azione all'interno dell'ODV ad eccezione della visualizzazione della documentazione interna delle API REST. Per l'autenticazione con l'ODV, gli utenti possono utilizzare uno dei seguenti metodi: autenticazione locale e autenticazione basata su directory.

- **Gestione della sicurezza**: l'ODV fornisce funzioni di gestione per le funzionalità relative alla sicurezza, inclusa la gestione di criteri di avviso, destinazioni di avviso, account, ruoli, metodi di autenticazione, sessioni di *mirroring* e *host* DSC. L'ODV crea l'utente AdminRole predefinito alla prima configurazione, ma è in grado di gestire qualsiasi ruolo definito dall'amministratore creato dagli utenti dell'ODV.

- **Protezione del TSF**: l'ODV mantiene uno stato sicuro in caso di guasto di un nodo PSM. Mentre un nodo è inattivo, l'ODV fornisce comunque tutte le sue funzionalità. L'ODV fornisce marche temporali affidabili utilizzando l'orologio del sistema, che viene sincronizzato con un server NTP.

- **Utilizzo delle risorse**: l'ODV garantisce l'erogazione di tutte le sue funzionalità durante lo stato di guasto di un nodo PSM.

- **Accesso all'ODV**: quando utilizzano l'interfaccia utente Web dell'ODV, gli utenti dell'ODV hanno la possibilità di terminare la propria sessione facendo clic sul collegamento di disconnessione (*sign out*).

- **Percorsi e canali attendibili**: l'ODV fornisce canali attendibili tra sé stesso e il server AD/OpenLDAP nell'ambiente operativo mediante connessioni TLS. L'ODV fornisce anche percorsi affidabili tra sé stesso e gli utenti dell'ODV remoti utilizzando connessioni TLS per proteggere l'autenticazione e tutte le attività relative al TSF.

7.4 Documentazione

La documentazione specificata in Appendice A – Indicazioni per l'uso sicuro del prodotto, viene fornita al cliente insieme al prodotto.

La documentazione indicata contiene le informazioni richieste per l'inizializzazione, la configurazione e l'utilizzo sicuro dell'ODV in accordo a quanto specificato nel Traguardo di Sicurezza [TDS].

Devono inoltre essere seguite le ulteriori raccomandazioni per l'utilizzo sicuro dell'ODV contenute nel par. 8.2 di questo rapporto.

7.5 Conformità a Profili di Protezione

Il Traguardo di Sicurezza [TDS] non dichiara conformità ad alcun Profilo di Protezione.

7.6 Requisiti funzionali e di garanzia

Tutti i Requisiti di Garanzia (SAR) sono stati selezionati dai CC Parte 3 [CC3].

Tutti i Requisiti Funzionali di Sicurezza (SFR) sono stati derivati direttamente dai CC Parte 2 [CC2].

Il Traguardo di Sicurezza [TDS], a cui si rimanda per la completa descrizione e le note applicative, specifica per l'ODV tutti gli obiettivi di sicurezza, le minacce che questi obiettivi devono contrastare, gli SFR e le funzioni di sicurezza che realizzano gli obiettivi stessi.

7.7 Conduzione della valutazione

La valutazione è stata svolta in conformità ai requisiti dello Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione, come descritto nelle Linee Guida Provvisorie [LGP3] e nelle Note Informative dello Schema [NIS3], ed è stata inoltre condotta secondo i requisiti del Common Criteria Recognition Arrangement [CCRA].

Lo scopo della valutazione è quello di fornire garanzie sull'efficacia dell'ODV nel soddisfare quanto dichiarato nel rispettivo Traguardo di Sicurezza [TDS], di cui si raccomanda la lettura ai potenziali acquirenti. Inizialmente è stato valutato il Traguardo di Sicurezza per garantire che costituisse una solida base per una valutazione nel rispetto dei requisiti espressi dallo standard CC. Quindi è stato valutato l'ODV sulla base delle dichiarazioni formulate nel Traguardo di Sicurezza stesso. Entrambe le fasi della valutazione sono state condotte in conformità ai CC Parte 3 [CC3] e alla CEM [CEM].

L'Organismo di Certificazione ha supervisionato lo svolgimento della valutazione eseguita dall'LVS CCLab Software Laboratory.

L'attività di valutazione è terminata in data 25 febbraio 2022 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione l'8 marzo 2022. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

7.8 Considerazioni generali sulla validità della certificazione

- La valutazione ha riguardato le funzionalità di sicurezza dichiarate nel Traguardo di Sicurezza [TDS], con riferimento all'ambiente operativo ivi specificato. La valutazione è stata eseguita sull'ODV configurato come descritto in Pensando Distributed Services Platform, Enterprise Edition Release Notes Version 1.28.0-E [DSPRN]

- Pensando Policy and Services Manager, Enterprise Edition User Guide [DSPUG]

- Pensando Policy and Services Manager LDAP Server Configuration Guide [DSPLDAP]

- Pensando Distributed Services Platform, Enterprise Edition Troubleshooting Guide [DSPTG]

- Pensando Policy and Services Manager, Enterprise Edition Design Best Practice Guide [DSPDBP]

- Pensando Distributed Services Card DSC-25 User Guide for Enterprise Edition [DSC25]

- Pensando Distributed Services Card DSC-100 User Guide for Enterprise Edition [DSC100]

- Pensando DSP Guidance Documentation Supplement [DSPGDS]

Appendice B – Configurazione valutata. I potenziali acquirenti sono invitati a verificare che questa corrisponda ai propri requisiti e a prestare attenzione alle raccomandazioni contenute in questo Rapporto di Certificazione.

La certificazione non è una garanzia di assenza di vulnerabilità; rimane una probabilità (tanto minore quanto maggiore è il livello di garanzia) che possano essere scoperte vulnerabilità sfruttabili dopo l'emissione del certificato. Questo Rapporto di Certificazione riflette le conclusioni dell'Organismo di Certificazione al momento della sua emissione. Gli acquirenti (potenziali e effettivi) sono invitati a verificare regolarmente l'eventuale insorgenza di nuove vulnerabilità successivamente all'emissione di questo Rapporto di Certificazione e, nel caso le vulnerabilità possano essere sfruttate nell'ambiente operativo dell'ODV, verificare presso il produttore se siano stati messi a punto aggiornamenti di sicurezza e se tali aggiornamenti siano stati valutati e certificati.

8 Esito della valutazione

8.1 Risultato della valutazione

- A seguito dell'analisi del Rapporto Finale di Valutazione [RFV] prodotto dall'LVS CCLab Software Laboratory e dei documenti richiesti per la certificazione, e in considerazione delle attività di valutazione svolte, come testimoniato dal gruppo di Certificazione, l'OCSI è giunto alla conclusione che l'ODV "Distributed Services Platform v1.28.0-E-96" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL2, con l'aggiunta di ALC_FLR.2, in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS] e nella configurazione valutata, riportata in Pensando Distributed Services Platform, Enterprise Edition Release Notes Version 1.28.0-E [DSPRN]

- Pensando Policy and Services Manager, Enterprise Edition User Guide [DSPUG]

- Pensando Policy and Services Manager LDAP Server Configuration Guide [DSPLDAP]

- Pensando Distributed Services Platform, Enterprise Edition Troubleshooting Guide [DSPTG]

- Pensando Policy and Services Manager, Enterprise Edition Design Best Practice Guide [DSPDBP]

- Pensando Distributed Services Card DSC-25 User Guide for Enterprise Edition [DSC25]

- Pensando Distributed Services Card DSC-100 User Guide for Enterprise Edition [DSC100]

- Pensando DSP Guidance Documentation Supplement [DSPGDS]

Appendice B – Configurazione valutata.

La Tabella 1 riassume i verdetti finali di ciascuna attività svolta dall'LVS in corrispondenza ai requisiti di garanzia previsti in [CC3], relativamente al livello di garanzia EAL2, con l'aggiunta di ALC_FLR.2.

Classi e componenti di garanzia		**Verdetto**
Security Target evaluation	**Classe ASE**	Positivo
Conformance claims	ASE_CCL.1	Positivo
Extended components definition	ASE_ECD.1	Positivo
ST introduction	ASE_INT.1	Positivo
Security objectives	ASE_OBJ.2	Positivo

Classi e componenti di garanzia		Verdetto
Derived security requirements	ASE_REQ.2	Positivo
Security problem definition	ASE_SPD.1	Positivo
TOE summary specification	ASE_TSS.1	Positivo
Development	**Classe ADV**	Positivo
Security architecture description	ADV_ARC.1	Positivo
Security-enforcing functional specification	ADV_FSP.2	Positivo
Basic design	ADV_TDS.1	Positivo
Guidance documents	**Classe AGD**	Positivo
Operational user guidance	AGD_OPE.1	Positivo
Preparative procedures	AGD_PRE.1	Positivo
Life cycle support	**Classe ALC**	Positivo
Use of a CM system	ALC_CMC.2	Positivo
Parts of the TOE CM coverage	ALC_CMS.2	Positivo
Delivery procedures	ALC_DEL.1	Positivo
Flaw reporting procedures	*ALC_FLR.2*	Positivo
Test	**Classe ATE**	Positivo
Evidence of coverage	ATE_COV.1	Positivo
Functional testing	ATE_FUN.1	Positivo
Independent testing - sample	ATE_IND.2	Positivo
Vulnerability assessment	**Classe AVA**	Positivo
Vulnerability analysis	AVA_VAN.2	Positivo

Tabella 1 - Verdetti finali per i requisiti di garanzia

8.2 Raccomandazioni

Le conclusioni dell'Organismo di Certificazione sono riassunte nel capitolo 5.1 (Dichiarazione di certificazione).

Si raccomanda ai potenziali acquirenti del prodotto "Distributed Services Platform v1.28.0-E-96" di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto in riferimento al Traguardo di Sicurezza [TDS].

L'ODV deve essere utilizzato in accordo agli Obiettivi di Sicurezza per l'ambiente operativo specificati nel par. 4.2 del Traguardo di Sicurezza [TDS]. Si assume che, nell'ambiente operativo in cui è posto in esercizio l'ODV, vengano rispettate le ipotesi descritte nel par. 3.3 del Traguardo di Sicurezza [TDS].

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella sua configurazione valutata. In particolare, l'Appendice A – Indicazioni per l'uso sicuro del prodotto del presente Rapporto include una serie di raccomandazioni relative alla consegna, all'inizializzazione, all'installazione e all'utilizzo sicuro del prodotto, in accordo con la documentazione di guida fornita con l'ODV ([DSPRN], [DSPUG], [DSPLDAP], [DSPTG], [DSPDBP], [DSC25], [DSC100], [DSPGDS]).

9 Appendice A – Indicazioni per l'uso sicuro del prodotto

La presente appendice riporta considerazioni particolarmente rilevanti per il potenziale acquirente del prodotto.

9.1 Consegna dell'ODV

L'ODV include il firmware Distributed Services Card (DSC) v1.28.0-E-96, il software Policy and Services Manager (PSM) v1.28.0-E-96 e la documentazione di guida elencata nella par. 9.3.

Il Fornitore dell'ODV, Pensando Systems, Inc., distribuisce il firmware DSC ai clienti tramite pacchetti fisici ed elettronici, mentre il software PSM viene fornito solo in formato elettronico.

Per quanto riguarda la distribuzione fisica, le schede DSC vengono imballate presso il sito di produzione. Su ogni DSC viene installato il firmware DSC e questi vengono quindi inseriti singolarmente in un sacchetto antistatico. Ogni scatola pronta per la spedizione contiene dodici schede così imbustate. Su ciascuna scheda DSC viene posta un'etichetta con le informazioni sul prodotto e l'indirizzo MAC. Le informazioni sul prodotto vengono anche stampate su un'etichetta posta sulla scatola. I clienti ritirano le schede DSC acquistate mediante un vettore di trasporto di propria scelta inviato presso lo stabilimento di Pensando.

Per la distribuzione elettronica, sia il firmware DSC, sia il software PSM sono disponibili ai clienti separatamente in file con estensione ".tgz" da scaricare dal Pensando Support Portal (è necessario un account per accedere al portale). Anche la documentazione dell'ODV può essere scaricata dal Pensando Support Portal.

9.2 Identificazione dell'ODV

Il software, il firmware e la documentazione dell'ODV sono dotati di una versione univoca per una facile identificazione.

Quando ricevono l'hardware fisico, i clienti devono come prima cosa verificare le informazioni di tracciamento del proprio ordine. I clienti dovranno inoltre controllare le etichette dei prodotti sulle scatole per verificare la correttezza dei prodotti ricevuti e la corrispondenza dei numeri di serie.

Quando si ricevono i componenti dell'ODV elettronicamente, occorre verificare che i file ".tgz" non siano stati manomessi verificando i rispettivi *checksum* SHA-256. I *checksum* sono disponibili assieme i file nella pagina di download del Pensando Support Portal.

Per confermare la versione corretta dell'ODV dopo l'installazione, il cliente può visualizzare la versione del software PSM dalla Web UI cliccando sull'icona "Information" in alto a destra e selezionando l'opzione "About". Le informazioni sulla versione sono elencate come "Build Version". Per visualizzare la versione del firmware DSC, occorre fare clic sul menu "System" a sinistra e selezionare il sottomenu "DSC". Le informazioni sulla versione sono elencate nella tabella "Distributed Services Cards" nella colonna "Version".

9.3 Installazione, inizializzazione e utilizzo sicuro dell'ODV

L'installazione, la configurazione e l'operatività dell'ODV devono essere eseguite secondo le istruzioni riportate nelle sezioni appropriate della documentazione di guida fornita con il prodotto al cliente.

In particolare, i seguenti documenti contengono informazioni dettagliate per l'inizializzazione sicura dell'ODV, la preparazione del suo ambiente operativo e il funzionamento sicuro dell'ODV in conformità con gli obiettivi di sicurezza specificati nel Traguardo di Sicurezza [TDS]:

- Pensando Distributed Services Platform, Enterprise Edition Release Notes Version 1.28.0-E [DSPRN]
- Pensando Policy and Services Manager, Enterprise Edition User Guide [DSPUG]
- Pensando Policy and Services Manager LDAP Server Configuration Guide [DSPLDAP]
- Pensando Distributed Services Platform, Enterprise Edition Troubleshooting Guide [DSPTG]
- Pensando Policy and Services Manager, Enterprise Edition Design Best Practice Guide [DSPDBP]
- Pensando Distributed Services Card DSC-25 User Guide for Enterprise Edition [DSC25]
- Pensando Distributed Services Card DSC-100 User Guide for Enterprise Edition [DSC100]
- Pensando DSP Guidance Documentation Supplement [DSPGDS]

10 Appendice B – Configurazione valutata

L'oggetto della valutazione (ODV) è il prodotto "Distributed Services Platform v1.28.0-E-96", sviluppato dalla società Pensando Systems, Inc.

Il nome e il numero di versione identificano in modo univoco l'ODV e i suoi componenti, che costituiscono la configurazione valutata dell'ODV verificata dai Valutatori al momento dell'effettuazione dei test e alla quale si applicano i risultati della valutazione.

La configurazione valutata dell'ODV include i seguenti componenti:

- Pensando Distributed Services Card Firmware v1.28.0-E-96 in esecuzione sul chip Capri presente sulle schede DSC-25 e DSC-100 installate su server separati nell'ambiente operativo.
- Pensando Policy and Services Manager v1.28.0-E-96 in esecuzione su un cluster di tre nodi installato su macchine virtuali nell'ambiente operativo.

Le seguenti funzionalità non fanno parte della configurazione valutata dell'ODV:

- funzionalità fornita dal driver DSC sul sistema operativo della macchina *host*;
- funzionalità coperte unicamente dal contratto di servizio Enterprise Pro;
- autenticazione RADIUS.

10.1 Ambiente operativo dell'ODV

Per il suo corretto funzionamento l'ODV necessita di specifiche risorse nell'ambiente operativo. Per ospitare il cluster PSM, nell'ambiente operativo deve essere disponibile un server *host* dedicato su cui è in esecuzione un *hypervisor* su cui sono caricate le tre VM dei nodi PSM. Per eseguire il firmware DSC, sono necessarie le schede DSC-25 e DSC-100, che vengono installate in server *host* separati nell'ambiente operativo.

Per eseguire alcune funzionalità l'ODV necessita anche di server esterni, tra cui un server NTP per la sincronizzazione dell'ora, un server AD o OpenLDAP per l'autenticazione basata su directory e la risoluzione dei gruppi espansi e un server *syslog* per la ricezione di avvisi.

Per la gestione dell'ODV, gli utenti abilitati potranno anche utilizzare una workstation nell'ambiente operativo collegata al cluster PSM.

Per maggiori dettagli sui requisiti minimi hardware e software dell'ambiente operativo dell'ODV si consulti il par. 1.5 del Traguardo di Sicurezza [TDS].

11 Appendice C – Attività di Test

Questa appendice descrive l'impegno dei Valutatori e del Fornitore nelle attività di test. Per il livello di garanzia EAL2, con l'aggiunta di ALC_FLR.2, tali attività tali attività prevedono tre passi successivi:

- valutazione dei test eseguiti dal Fornitore in termini di copertura;
- esecuzione di test funzionali indipendenti da parte dei Valutatori;
- esecuzione di test di intrusione da parte dei Valutatori.

11.1 Configurazione per i Test

I Valutatori hanno eseguito tutti i casi di test sull'ambiente di test messo a disposizione dal Fornitore assieme a tutte le risorse necessarie per le attività di test.

L'ambiente di test dell'ODV è stato predisposto e configurato sulla base della documentazione di test del Fornitore. La versione valutata dell'ODV è stata installata in un cluster di tre nodi utilizzando macchine virtuali in esecuzione su un sistema VMware ESXi. Il firmware delle Distributed Services Card di Pensando era in esecuzione sul chip Capri presente su una scheda DSC-25 e una scheda DSC-100 installate su server separati. L'ambiente di test era composto dai seguenti elementi:

- un computer per uso generico con installato Kali Linux 2021.3 Release;
- un server con installato un *hypervisor* VMware ESXi versione 6.7.0 (Dell PowerEdge R640);
- una scheda DSC-25 e una scheda DSC-100 installate su due server separati (Dell PowerEdge R640 e HPE ProLiant DL360);
- infrastruttura di rete;
- un server con installato Microsoft Windows Server 2019 Standard Edition che fornisce funzionalità NTP e *syslog collector* (Kiwi Syslog Server 9.7.2.1).

I Valutatori hanno installato l'ODV seguendo i passi descritti nel cap. 2.2 "Secure Installation" del documento [DSPGDS].

11.2 Test funzionali svolti dal Fornitore

11.2.1 Approccio adottato per i test

L'approccio del Fornitore ai test consiste nel predisporre un test funzionale specifico per ciascuna caratteristica comportamentale degli SFR dichiarati nel Traguardo di Sicurezza [TDS]. I test del Fornitore mirano alla copertura di tutte gli aspetti di sicurezza dell'ODV garantendo che la verifica funzionale sia completa senza essere inutilmente dettagliata.

La documentazione di test del Fornitore include un totale di 5 casi di test mappati sulle TSFI elencate nel documento di Specifiche Funzionali (Web UI e REST API).

Tutti le TSFI definite sono coperte dai seguenti casi di test:

- Caso di test 01 – Accesso dell'utente
- Caso di test 02 – Avvisi, eventi e eventi di audit
- Caso di test 03 – REST API
- Caso di test 04 – Connessioni sicure
- Caso di test 05 – Guasto di un nodo

I Valutatori hanno analizzato i test funzionali del Fornitore e la loro copertura riscontrandone la completezza ed accuratezza.

11.2.2 Risultati dei test

Nella documentazione di test del Fornitore, per ogni caso di test viene descritto lo scopo, le TSFI e gli SFR rilevanti, i prerequisiti necessari, le procedure passo-passo per la sua esecuzione e il risultato previsto.

I risultati effettivi ottenuti da tutti i test del Fornitore sono risultati conformi a quelli previsti.

11.3 Test funzionali ed indipendenti svolti dai Valutatori

11.3.1 Approccio adottato per i test

I Valutatori hanno eseguito tutti i test sull'ambiente di test messo a disposizione dal Fornitore. L'ambiente di test dell'ODV è stato predisposto secondo quanto descritto nel piano di test del Fornitore e nelle procedure preparatorie fornite nel documento [DSPGDS]. Prima di iniziare l'attività di test, i Valutatori hanno verificato che l'ambiente di test fosse stato predisposto in maniera appropriata e che l'ODV fosse configurato correttamente e si trovasse in uno stato noto.

I Valutatori hanno ripetuto tutti i passi per ciascuno dei casi di test del Fornitore e hanno verificato i risultati attesi.

Allo scopo di esercitare ulteriormente le TSFI REST API e Web UI, i Valutatori hanno progettato i seguenti casi di test aggiuntivi, derivati dai casi di test del Fornitore:

- Caso di test dei Valutatori 01 – Rispetto dei requisiti di complessità delle password
- Caso di test dei Valutatori 02 – Verifica dei messaggi di *syslog* con Wireshark
- Caso di test dei Valutatori 03 – Modifica del nodo leader

11.3.2 Risultati dei test

Tutti i test del Fornitore sono stati eseguiti con successo. I Valutatori hanno verificato il corretto comportamento delle TSFI e la corrispondenza tra risultati attesi e risultati ottenuti per ogni test.

Tutti i casi di test progettati dai Valutatori hanno avuto esito positivo, ovvero tutti i risultati dei test sono risultati conformi a quelli previsti.

11.4 Analisi delle vulnerabilità e test di intrusione

Per l'esecuzione di queste attività i Valutatori hanno lavorato sullo stesso ambiente di test dell'ODV già utilizzato per le attività dei test funzionali, verificando che la configurazione di test fosse congruente con la versione dell'ODV in valutazione.

In una prima fase, i Valutatori hanno condotto ricerche su fonti pubbliche per identificare potenziali vulnerabilità dell'ODV. Come risultato di questa attività, sono state identificate diverse vulnerabilità potenziali nel pacchetto Elasticsearch.

I Valutatori hanno esaminato queste vulnerabilità e hanno concluso che non sono applicabili all'ODV. Elasticsearch (porta 9200) viene utilizzato nell'ODV per lo scambio di dati tra i nodi del cluster PSM. Questa comunicazione è protetta da TLS con autenticazione basata su certificato e le porte aperte non sono raggiungibili dall'esterno dell'ODV.

I Valutatori hanno quindi condotto una ricerca sulle evidenze di valutazione, inclusi TDS, documentazione di guida, specifiche funzionali, progettazione dell'ODV e descrizione dell'architettura di sicurezza. Questa analisi ha rivelato le seguenti aree di interesse:

- Attacco a forza bruta alla pagina di accesso del PSM
- Esecuzione di codice da remoto nella funzionalità System Upgrade

I Valutatori hanno condotto test di intrusione per verificare l'effettiva sfruttabilità di queste vulnerabilità potenziali nell'ambiente operativo dell'ODV, considerando un potenziale d'attacco di livello Basic.

Sulla base dell'analisi di vulnerabilità e dei risultati dei test di intrusione, i Valutatori hanno stabilito che nessuna delle vulnerabilità potenziali identificate è applicabile all'ODV. L'ODV, nel suo ambiente operativo, è quindi in grado di resistere ad un attaccante che possiede un potenziale di attacco di livello Basic. Non sono state identificate vulnerabilità sfruttabili o residue.