PREMIER MINISTRE

Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

Secrétariat général de la défense et de la sécurité nationale

Rapport de certification ANSSI-CSPN-2025/04

Tanium

[Serveur de modules : 7.6.4.2065 Agents : 7.6.2.1259]

Paris, le 27 Mai 2025

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information

Vincent STRUBEL

[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

AVERTISSEMENT

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CSPN-2025/04

Nom du produit

Tanium

Référence/version du produit

[Serveur de modules : 7.6.4.2065 Agents : 7.6.2.1259]

Catégorie de produit

Administration et supervision de la sécurité

Critère d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)

Commanditaire

TANIUM
191/195 avenue Charles de Gaulle
92200, Neuilly-sur-Seine

Développeur

TANIUM
191/195 avenue Charles de Gaulle
92200, Neuilly-sur-Seine

Centre d'évaluation

LEXFO
5 rue Saulnier
75009 Paris

Accord de reconnaissance applicable

fixed time certification

Ce certificat est reconnu dans le cadre du [BSZ_CSPN]

Fonctions de sécurité évaluées

Identification, authentification et contrôle d'accès
Authentification des composants
Intégrité et chiffrement des échanges entre composants
Intégrité et chiffrement des échanges utilisateurs/serveur
Validation des entrées
Signature des mises à jour
Epinglage de certificats
Chiffrement du mot de passe du bootloader

Fonctions de sécurité non évaluées

Aucune

Restriction(s) d'usage

Non

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- l'Agence nationale de la sécurité des systèmes d'information élabore les rapports de certification. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7) ;
- les certificats délivrés par le directeur général de l'Agence nationale de la sécurité des systèmes d'information attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification CSPN sont disponibles sur le site Internet cyber.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « Tanium, [Serveur de modules : 7.6.4.2065 Agents : 7.6.2.1259] » développé par TANIUM.

Ce produit est destiné à être utilisé pour la gestion des vulnérabilités d'un parc informatique au sein des entreprises. Cette solution permet d'avoir une vue précise sur les composants du parc informatique, d'en retirer des métriques et d'effectuer directement des actions sur celui-ci. Composée de nombreux modules optionnels activés au choix des utilisateurs, elle permet notamment de :

- Inventorier la totalité des assets d'un parc ;
- répertorier et alerter sur les différents logiciels déployés sur le parc ;
- identifier l'activité des utilisateurs et des assets sur le parc ;
- investiguer les menaces actives sur le parc ;
- surveiller les performances des assets présents sur le parc ;
- déployer des logiciels et des mises-à-jour ;
- constater la santé du parc au travers de scans automatisés ;
- générer des rapports sur l'état du parc ;
- évaluer, monitorer et remédier le niveau de risque IT;
- vérifier et déployer des politiques à l'échelle du parc ;
- s'interfacer avec d'autres outils (CMDB, ITAM, ITSM, EDR, SIEM, SOAR, …)

1.2 Description du produit évalué

La cible de sécurité [CDS] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1 *Catégorie du produit*

☐	1	détection d'intrusions
☐	2	anti-virus, protection contre les codes malicieux
☐	3	pare-feu
☐	4	effacement de données
☒	5	**administration et supervision de la sécurité**
☐	6	identification, authentification et contrôle d'accès
☐	7	communication sécurisée
☐	8	messagerie sécurisée
☐	9	stockage sécurisé
☐	10	environnement d'exécution sécurisé
☐	11	terminal de réception numérique (*Set top box*, STB)
☐	12	matériel et logiciel embarqué
☐	13	automate programmable industriel
☐	99	autre

1.2.2 *Identification du produit*

Produit	
Nom du produit	Tanium
Numéro de la version évaluée	[Serveur de modules : 7.6.4.2065 Agents : 7.6.2.1259]

La version certifiée du produit peut être identifiée de la manière suivante :

- Via un navigateur web sur l'interface d'administration pour la partie module serveur ;
- Dans une console système, via la commande « TaniumClient –version » pour les agents installés sur les postes à superviser.

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- L'identification, authentification et contrôle d'accès ;
- l'authentification des composants ;
- l'intégrité et chiffrement des échanges entre les composants ;
- l'intégrité et le chiffrement des échanges entre les utilisateurs et le serveur ;
- la validation des entrées de données ;
- la signature des mises à jour assurant leur authenticité ;
- l'épinglage des certificats afin d'assurer la protection des communications ;
- le chiffrement du mot de passe du bootloader.

1.2.4 *Configuration évaluée*

La configuration évaluée correspond à celle décrite par la procédure d'installation officielle du produit.

La plateforme de test est constituée des éléments suivants :

- Deux machines virtuelles gérées par un hyperviseur Proxmox, l'une contenant le serveur Tanium, et l'autre contenant le serveur de module. Ces machines virtuelles ont été hébergées sur le matériel suivant :
  - *Dell PowerEdge* R650
  - 2x Intel Xeon Gold 6630 2.0Ghz, 28 *cores*/56 *Threads*
  - 512 Gb RAM
  - 2x 1.5TB de stockage en RAID1
  - 20x 2.4 TB de stockage en SAS
- Deux agents installés sur deux machines virtuelles distinctes sous GNU/Linux et Windows ;
- Un agent installé sur un ordinateur Apple sous Mac OS X.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN].

2.2 Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, des menaces, des utilisateurs et des fonctions de sécurité définis dans la cible de sécurité [CDS].

2.2.1 *Installation du produit*

2.2.1.1 Particularités de paramétrage de l'environnement et options d'installation

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

2.2.1.2 Description de l'installation et des non-conformités éventuelles

Ayant suivi la procédure d'installation officielle du produit, l'évaluateur n'a identifié aucune non-conformité pendant cette phase d'installation et de mise en œuvre.

2.2.1.3 Notes et remarques diverses

Pendant l'installation, l'utilisateur peut utiliser des paramètres qui réduiront la sécurité du produit, cependant, la documentation avertit l'utilisateur des risques de réduction du niveau de sécurité en cas d'utilisation de certains paramètres. Si la documentation est strictement suivie, aucune réduction du niveau de sécurité du produit ne se produira.

2.2.2 *Analyse de la documentation*

Les guides du produit permettent d'installer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

2.2.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source de l'implémentation des mécanismes cryptographiques du produit.

Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

2.2.4 *Analyse de la conformité des fonctions de sécurité*

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

2.2.5 *Analyse de la résistance des mécanismes des fonctions de sécurité*

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

2.2.6 *Analyse des vulnérabilités (conception, construction, etc.)*

2.2.6.1 Liste des vulnérabilités connues

Des vulnérabilités publiques existent sur le produit ou sur ses briques logicielles tierces, mais se sont révélées inexploitables, soit pour le niveau d'attaquant considéré, soit dans le contexte défini par la cible de sécurité [CDS].

2.2.6.2 Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Il n'a pas été découvert de vulnérabilité propre au produit, ni dans son implémentation, qui puisse remettre en cause la sécurité du produit.

2.2.7 *Analyse de la facilité d'emploi*

2.2.7.1 Cas où la sécurité est remise en cause

L'évaluateur n'a pas identifié de cas où la sécurité de la TOE est remise en cause.

2.2.7.2 Avis d'expert sur la facilité d'emploi

Aucun avis d'expert du CESTI n'a été donné quant à la facilité d'emploi du produit.

2.2.7.3 Notes et remarques diverses

Une non-conformité à l'état de l'art relative à l'utilisation de SHA-224 au sein du mécanisme de signature pour TLS a été identifiée. Cette non-conformité ne représente cependant pas un risque de sécurité.

Différents composants utilisés par le produit sont sujet à des vulnérabilités publiques non exploitables dans le contexte prévu par la cible de sécurité [CDS].

Un composant (libexpat) est sujet à des vulnérabilités dont la cotation les porte à être considérées comme résiduelles étant donné le niveau d'attaquant considéré.

2.3 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [CDS]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [RTE].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

2.4 Analyse du générateur d'aléa

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé. Afin que les mécanismes analysés soient conformes aux exigences de ce référentiel, les recommandations identifiées [GUIDES] doivent être suivies.

3 La certification

3.1 Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « Tanium, [Serveur de modules : 7.6.4.2065 Agents : 7.6.2.1259] » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

3.2 Recommandations et restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement spécifiés dans la cible de sécurité [CDS], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

3.3 Reconnaissance du certificat

Ce certificat est émis dans les conditions du [BSZ_CSPN].

Cet accord permet la reconnaissance mutuelle des certificats de sécurité pour les schémas CSPN (Certification de Sécurité de Premier Niveau) et BSZ *(Beschleunigte Sicherheitszertifizierung* ou Certification de sécurité accélérée).

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - Cible de sécurité CSPN Tanium , référence TAN20230602, version 1.5, 16 avril 2025.
[RTE]	Rapport technique d'évaluation : - *Technical Report CSPN Assessment*, référence TAN20250310, version 1.3, 25 avril 2025.
[GUIDES]	Guides du produit : - Documentation officielle en ligne https://help.tanium.com (lien vérifié en date du 7 mai 2025)

ANNEXE B. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01, version 5.0, 12 janvier 2023. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 5.0, 12 juillet 2024. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 4.0, 12 Juillet 2024.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1, 26 janvier 2021.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.
[BSZ_CSPN]	*Mutual Recognition Agreement of cybersecurity evaluation certificates issued under fixed time certification process, BSI/ANSSI,* référence *bsz_cspn_mutual_recognition_agreement,version* 2.0, mai 2024.