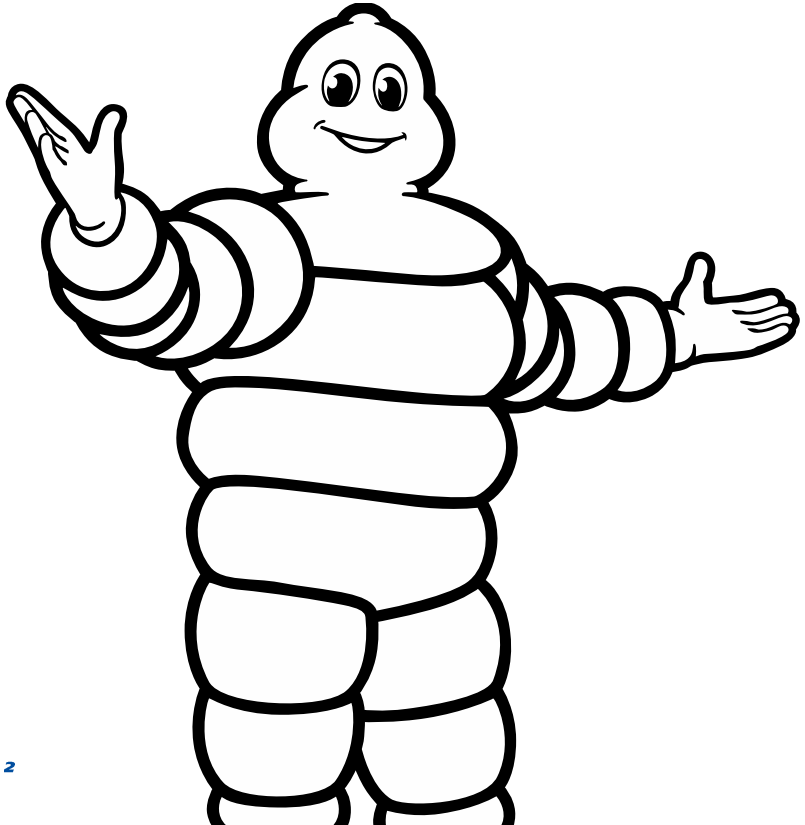
SÉCURISER LES BASES DE DONNÉES : DE L'AUDIT À L'ACTION AVEC LES RECOMMANDATIONS CIS

ALEXY MACE ET JEAN-LUC BENHAIM

MICHELIN

SOMMAIRE



DATABASE PLATFORM (DBPF)

- C’est une SQUAD dans le service Infrastructure composée d’experts
- Définition des normes et standards
- PostgreSQL, Oracle, MongoDB et SnowFlake
- Gestion du cycle de vie des produits (création => obsolescence)
- Aide à la décision
- Support aux équipes
- Automatisation

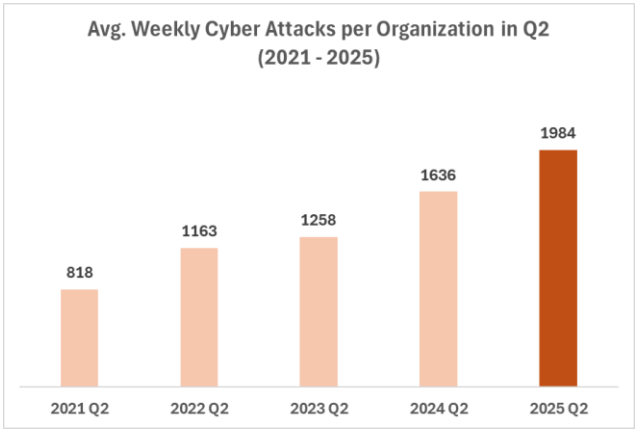
MICHELIN

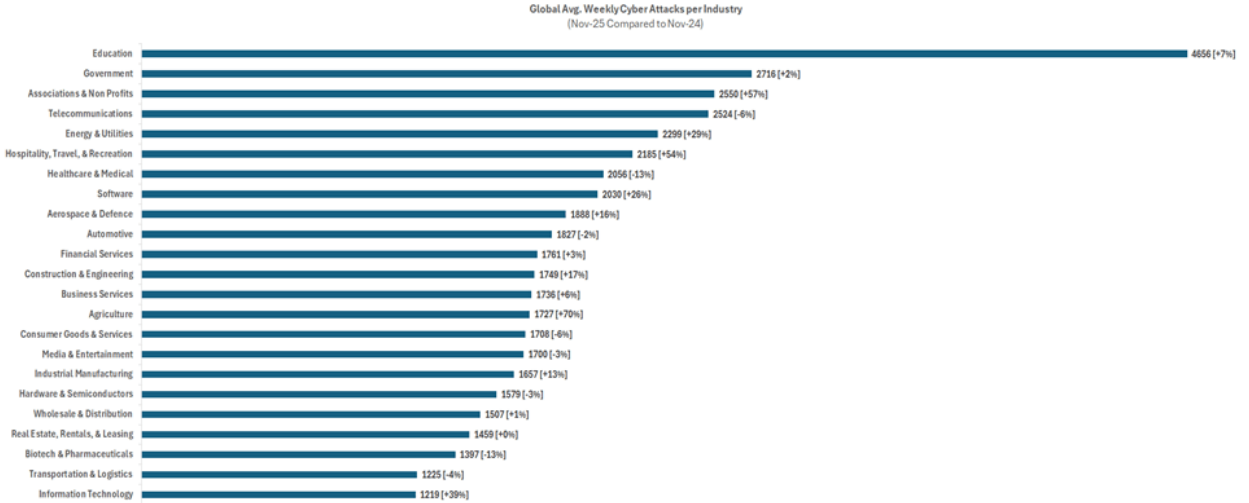
POSTGRESQL DANS LA DBPF

- EDB pour les instances On-Prem et Azure Flexible Server pour le communautaire
- PostgreSQL est la cible pour les nouveaux projets
- Migrations Oracle => PostgreSQL
- Migrations des modèles de données et des applications
- Expertise

MICHELIN

CONTEXTE

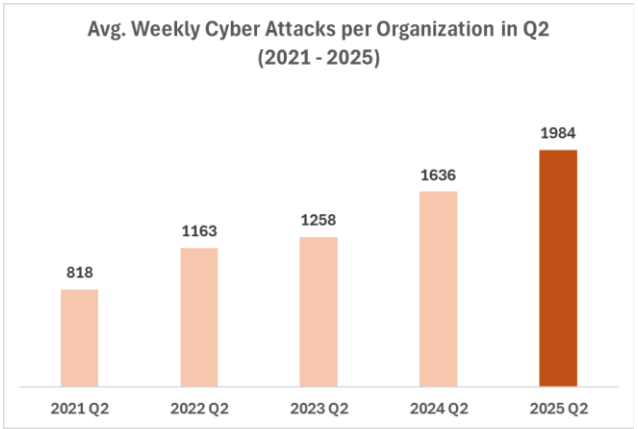


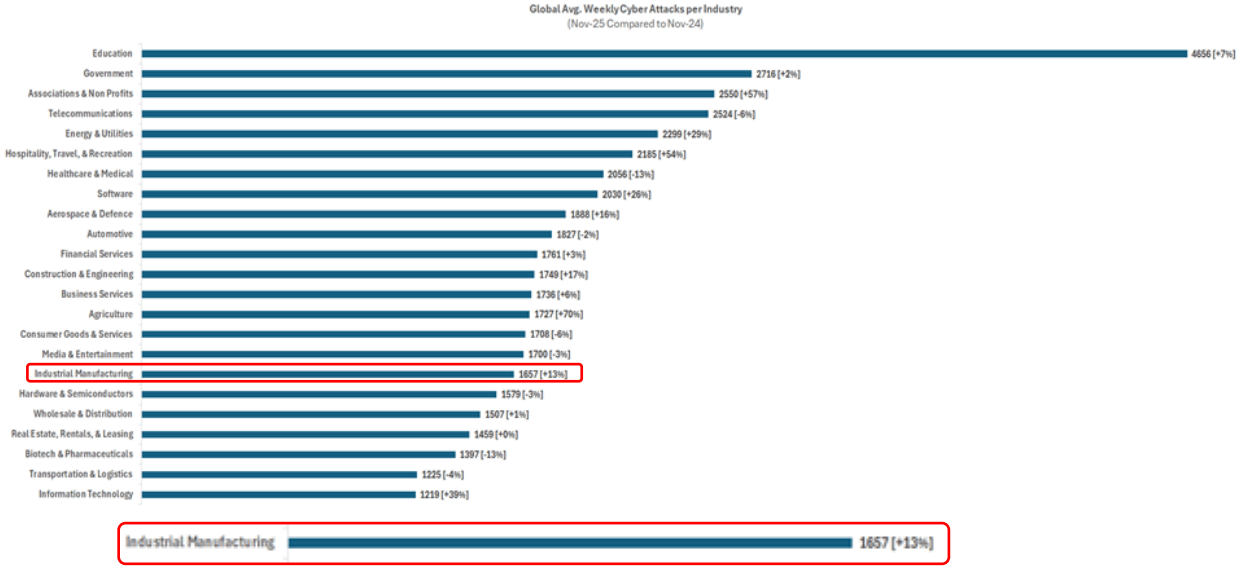


Source: checkpoint.com, a closer look at q2 2025 75 surge in cyber attacks worldwide

MICHELIN

CONTEXTE

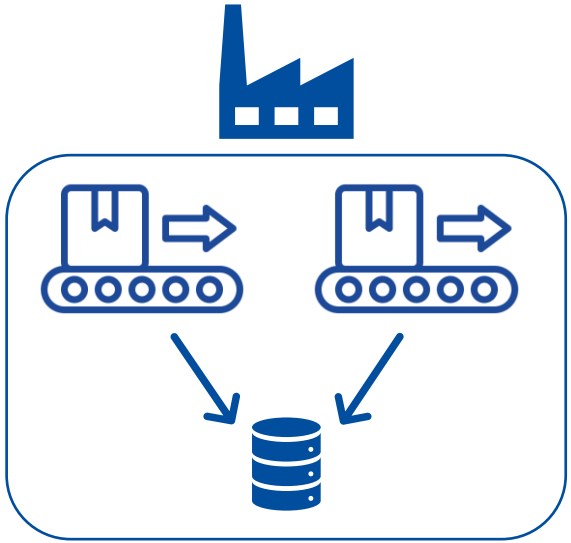




Source: checkpoint.com, a closer look at q2 2025 75 surge in cyber attacks worldwide

MICHELIN

CONTEXTE



COMMENT AMÉLIORER LA SÉCURITÉ DES BASES DE DONNÉES POSTGRESQL?

MICHELIN

INTRODUCTION AUX STANDARDS CIS

CIS Center for Internet Security®

- Organisation à but non lucratif
- Elabore des recommandations et des standards pour renforcer la sécurité des systèmes informatiques et réseaux
- Recommandations élaborées par des experts de la cybersécurité et une communauté collaborative
- Reconnus à l'international comme normes de sécurité pour la protection des SI et des données contre les cyberattaques

MICHELIN

LANCEMENT ET INTERPRÉTATION DES BENCHMARKS

CIS-CAT®Pro

Solution sous licence proposée par CIS Workbench

- **Facilité de lancement de scan sur 1 DB**
- **Configuration complexe pour automatisation**

tenable

Solution sous licence d'analyse de sécurité de systèmes on premise

- **Facilité de configuration pour scan multiple DB et multiple version**
- **Ne convient pas à un environnement Cloud**

KloudDB

Solution open source offrant une partie des benchmarks PostgreSQL

- **Solution gratuite**
- **Ne contient qu'un nombre limité de benchmarks**

orca security

Solution sous licence d'analyse de sécurité de systèmes cloud

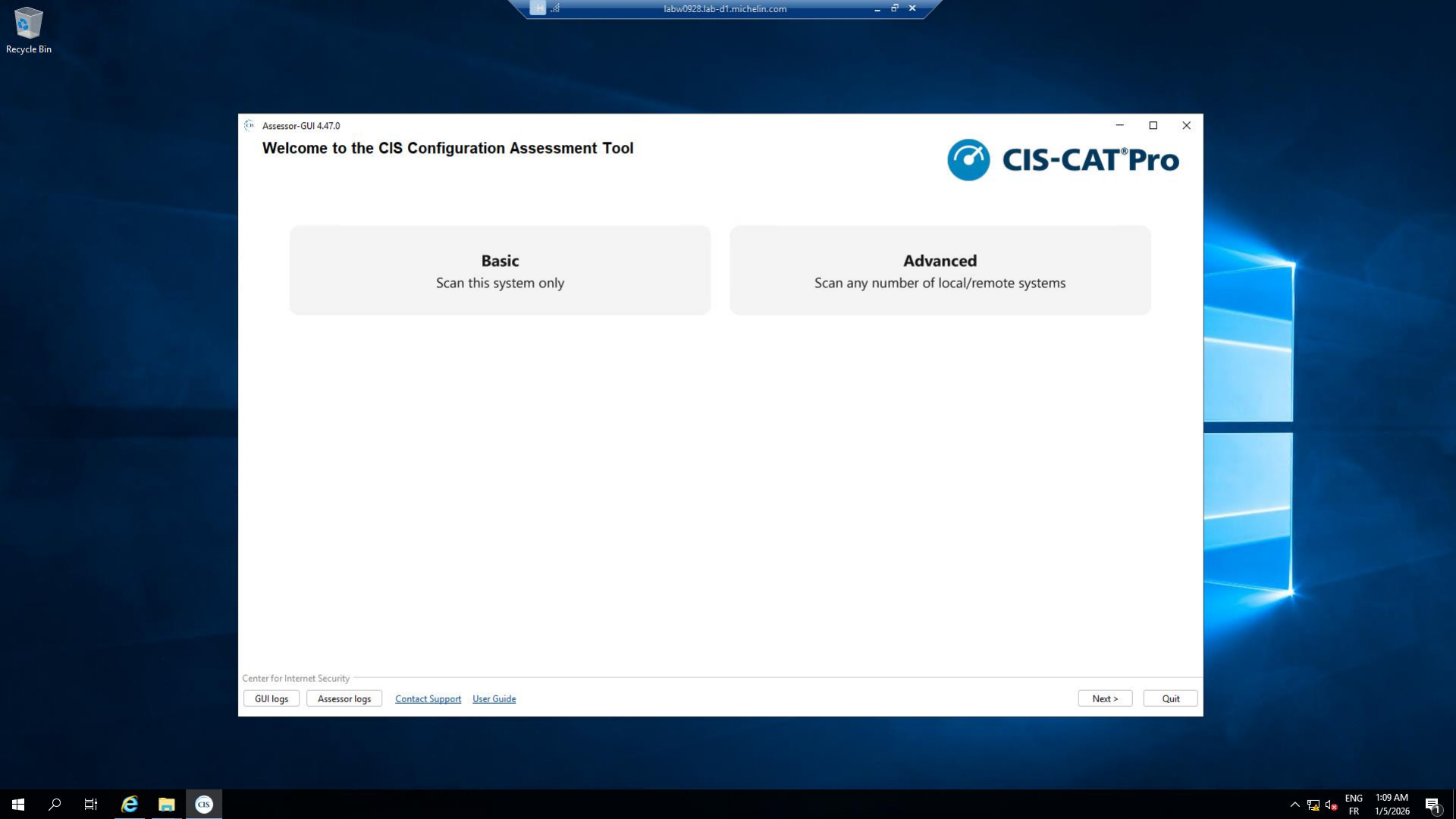
- **Facilité de configuration pour scan multiple DB et multiple version**
- **Ne convient pas à un environnement on premise**

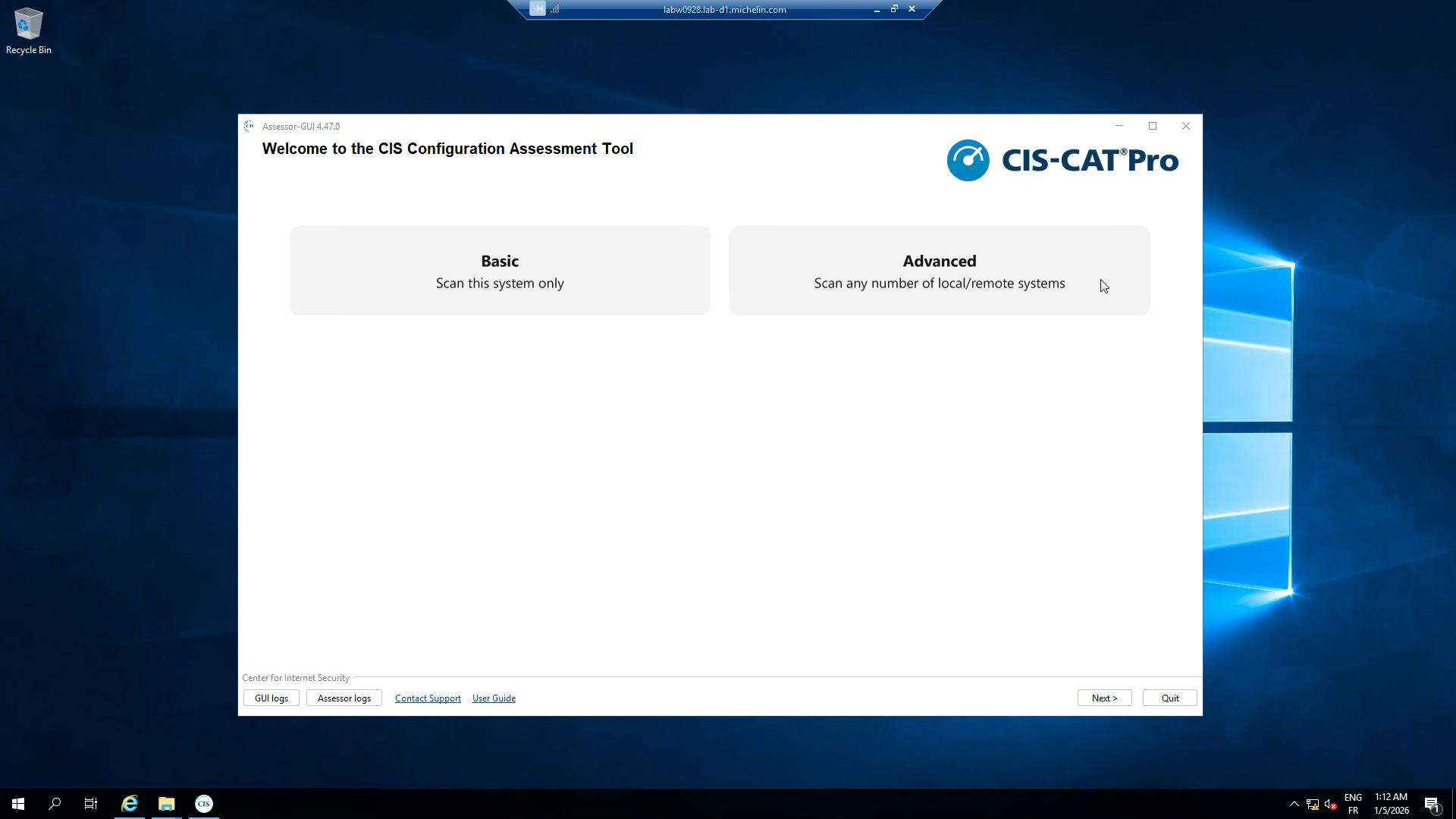
MICHELIN

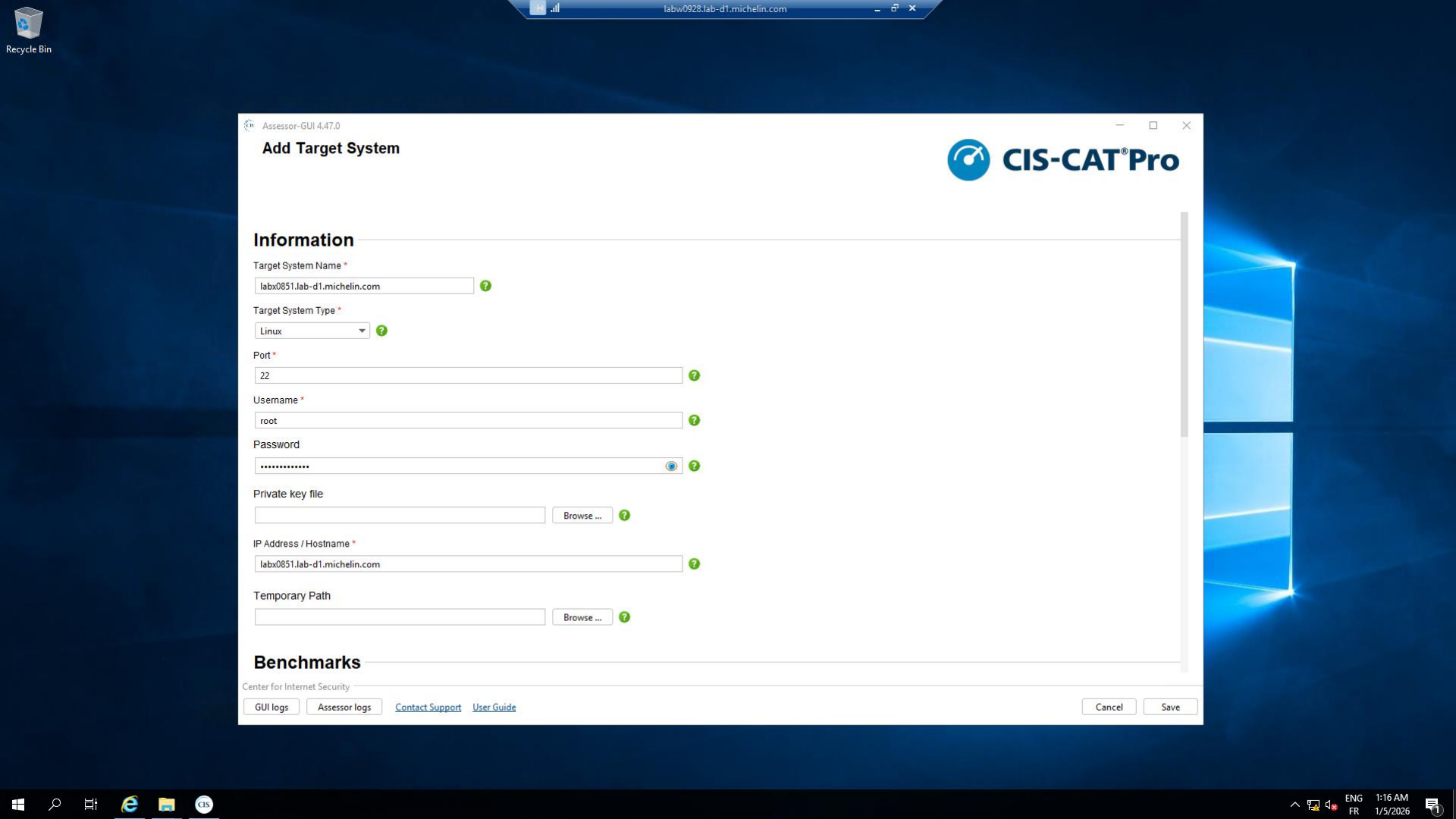
DÉMONSTRATION AVEC CIS CAT PRO

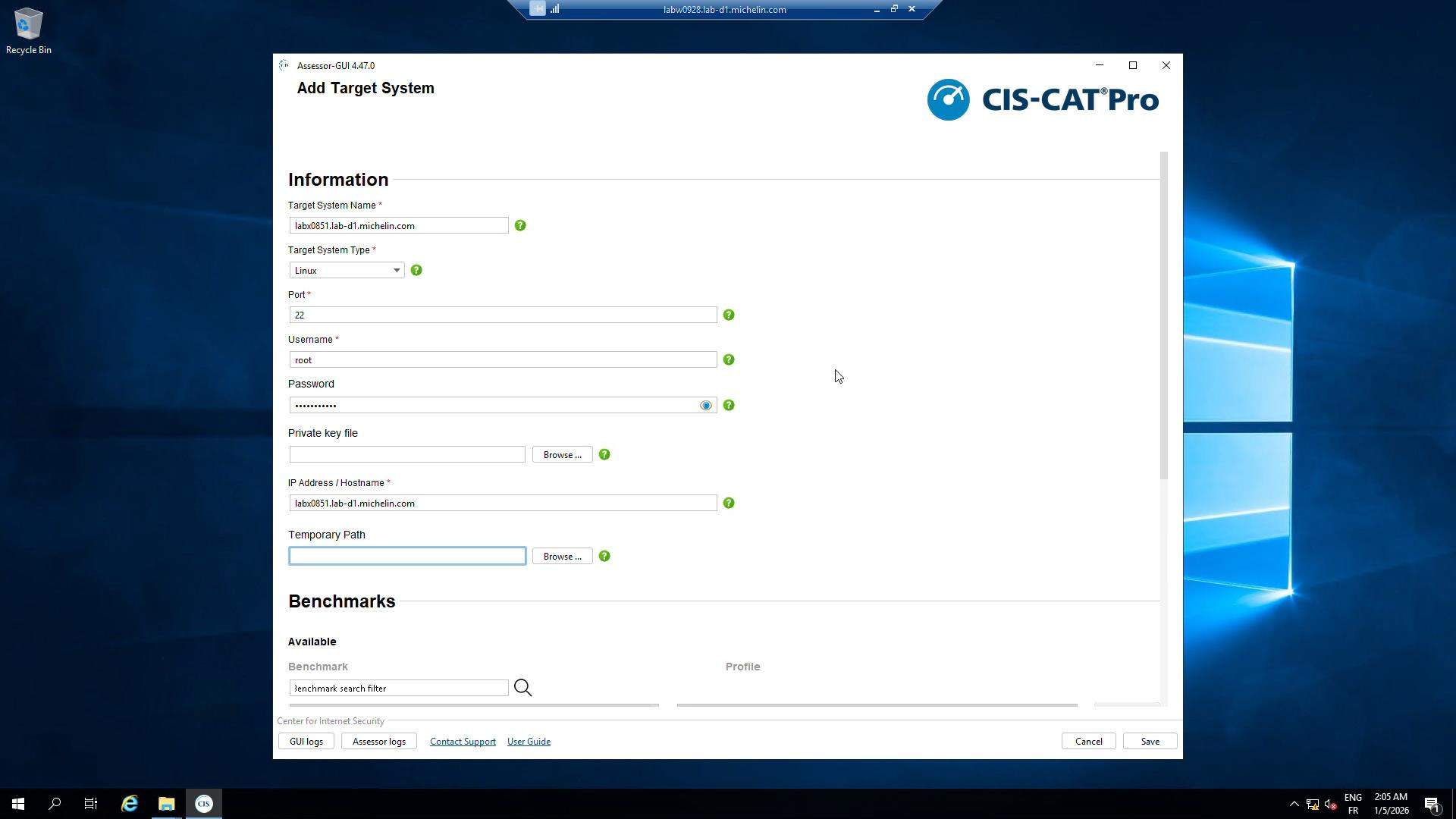
- 1 machine Linux
- 1 machine Windows
- 1 base PostgreSQL EDB 14
- CIS CAT Pro Assessor

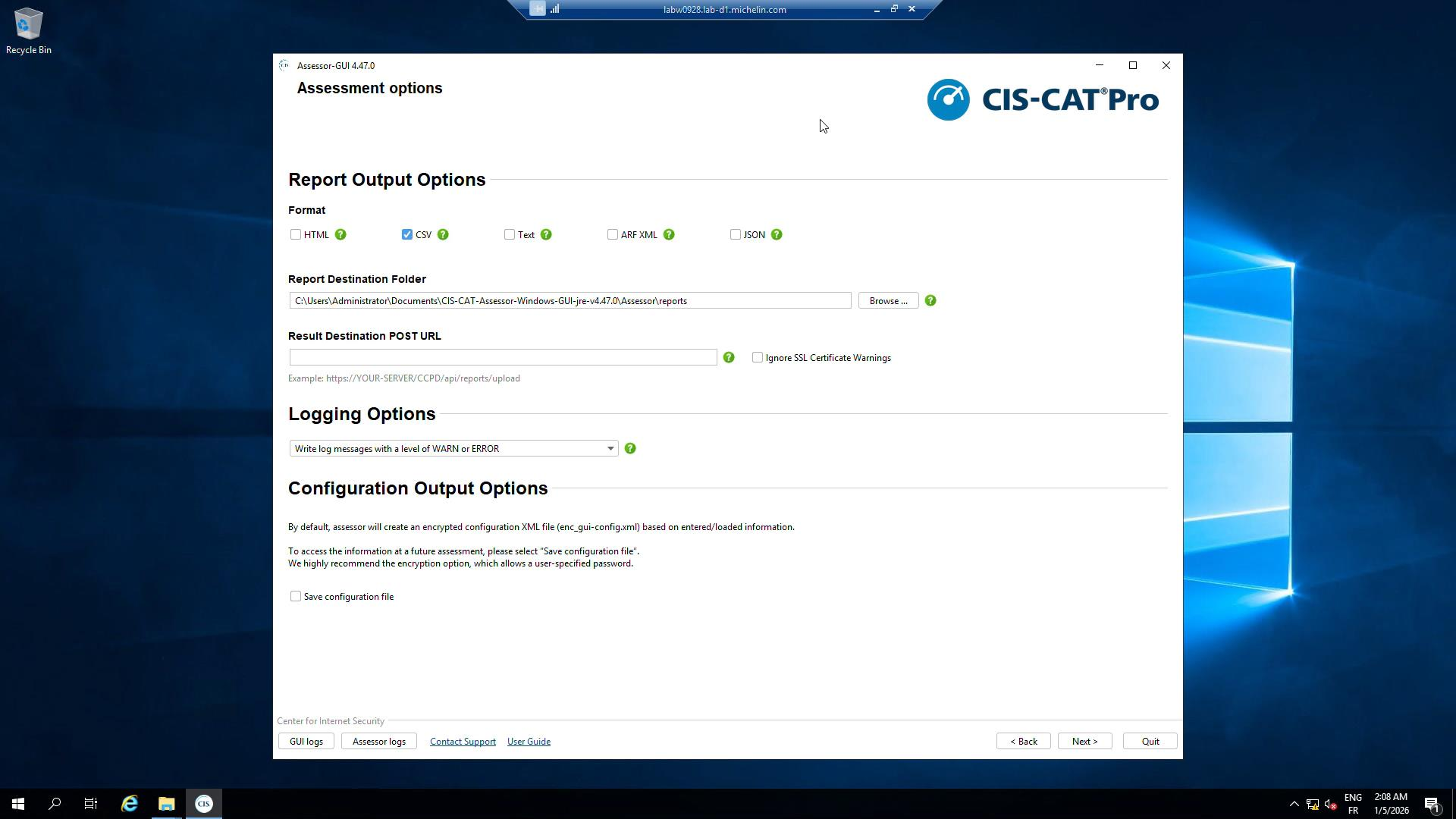
MICHELIN


labw0928.lab-d1.michelin.com
Recycle Bin
Assessor-GUI 4.47.0
Welcome to the CIS Configuration Assessment Tool
CIS-CAT Pro
Basic
Scan this system only
Advanced
Scan any number of local/remote systems
Center for Internet Security
GUI logs
Assessor logs
Contact Support
User Guide
Next >
Quit
ENG
FR
1:09 AM
1/5/2026


labw0928.lab-d1.michelin.com
Recycle Bin
Assessor-GUI 4.47.0
Welcome to the CIS Configuration Assessment Tool
CIS-CAT® Pro
Basic
Scan this system only
Advanced
Scan any number of local/remote systems
Center for Internet Security
GUI logs
Assessor logs
Contact Support
User Guide
Next >
Quit
ENG
FR
1:12 AM
1/5/2026


labw0928.lab-d1.michelin.com
Recycle Bin
Assessor-GUI 4.47.0
Add Target System
CIS-CAT Pro
Information
Target System Name *
labx0851.lab-d1.michelin.com
Target System Type *
Linux
Port *
22
Username *
root
Password
Private key file
Browse ...
IP Address / Hostname *
labx0851.lab-d1.michelin.com
Temporary Path
Browse ...
Benchmarks
Center for Internet Security
GUI logs
Assessor logs
Contact Support
User Guide
Cancel
Save
ENG
FR
1:16 AM
1/5/2026


labw0928.lab-d1.michelin.com
Recycle Bin
Assessor-GUI 4.47.0
Add Target System
CIS-CAT Pro
Information
Target System Name *
labx0851.lab-d1.michelin.com
Target System Type *
Linux
Port *
22
Username *
root
Password
Private key file
Browse ...
IP Address / Hostname *
labx0851.lab-d1.michelin.com
Temporary Path
Browse ...
Benchmarks
Available
Benchmark
Profile
Benchmark search filter
Center for Internet Security
GUI logs
Assessor logs
Contact Support
User Guide
Cancel
Save
ENG
FR
2:05 AM
1/5/2026


labw0928.lab-d1.michelin.com
Recycle Bin
Assessor-GUI 4.47.0
Assessment options
CIS-CAT Pro
Report Output Options
Format
HTML
CSV
Text
ARF XML
JSON
Report Destination Folder
C:\Users\Administrator\Documents\CIS-CAT-Assessor-Windows-GUI-jre-v4.47.0\Assessor\reports
Browse ...
Result Destination POST URL
Ignore SSL Certificate Warnings
Example: https://YOUR-SERVER/CCPD/api/reports/upload
Logging Options
Write log messages with a level of WARN or ERROR
Configuration Output Options
By default, assessor will create an encrypted configuration XML file (enc_gui-config.xml) based on entered/loaded information.
To access the information at a future assessment, please select "Save configuration file".
We highly recommend the encryption option, which allows a user-specified password.
Save configuration file
Center for Internet Security
GUI logs
Assessor logs
Contact Support
User Guide
< Back
Next >
Quit
ENG
FR
2:08 AM
1/5/2026

Description	Tests						Scoring		
	Pass	Fail	Error	Unkn.	Man.	Exc.	Score	Max	Percent
1 Installation and Patches	0	1	1	0	5	0	0.0	2.0	0%
2 Directory and File Permissions	0	0	0	0	4	0	0.0	0.0	0%
3 Logging And Auditing	17	8	0	0	1	0	17.0	25.0	68%
3.1 PostgreSQL Logging	17	7	0	0	1	0	17.0	24.0	71%
3.1.1 Logging Rationale	0	0	0	0	0	0	0.0	0.0	0%
4 User Access and Authorization	1	1	0	0	7	0	1.0	2.0	50%
5 Connection and Login	0	0	0	0	6	0	0.0	0.0	0%
6 PostgreSQL Settings	1	3	1	0	6	0	1.0	5.0	20%
7 Replication	0	0	1	0	4	0	0.0	1.0	0%
8 Special Configuration Considerations	1	0	0	0	2	0	1.0	1.0	100%
Total	20	13	3	0	35	0	20.0	36.0	56%

Score des recommandations automatiques

Recommandations manuelles

Score n'incluant pas les recommandations manuelles

MICHELIN

ANALYSE DES RÉSULTATS

Description	Tests						Scoring		
	Pass	Fail	Error	Unkn.	Man.	Exc.	Score	Max	Percent
1 Installation and Patches	0	1	1	0	5	0	0.0	2.0	0%
2 Directory and File Permissions	0	0	0	0	4	0	0.0	0.0	0%
3 Logging And Auditing	17	8	0	0	1	0	17.0	25.0	68%
3.1 PostgreSQL Logging	17	7	0	0	1	0	17.0	24.0	71%
3.1.1 Logging Rationale	0	0	0	0	0	0	0.0	0.0	0%
4 User Access and Authorization	1	1	0	0	7	0	1.0	2.0	50%
5 Connection and Login	0	0	0	0	6	0	0.0	0.0	0%
6 PostgreSQL Settings	1	3	1	0	6	0	1.0	5.0	20%
7 Replication	0	0	1	0	4	0	0.0	1.0	0%
8 Special Configuration Considerations	1	0	0	0	2	0	1.0	1.0	100%
Total	20	13	3	0	35	0	20.0	36.0	56%

Note: Actual scores are subject to rounding errors. The sum of these values may not result in the exact overall score.

The 'Exc' column only applies to Exceptions that are generated using CIS-CAT Pro Dashboard and is not utilized by CIS-CAT Pro Assessor.

Profiles

This benchmark contains 2 profiles.The **Level 1 - PostgreSQL on Linux** profile was used for this assessment.

Title	Description
Level 1 - PostgreSQL	Items in this profile apply to PostgreSQL 14 and intend to: • be practical and prudent; • provide a clear security benefit; and • not inhibit the utility of the technology beyond acceptable means. **Note:** The intent of this profile is to include checks that can be assessed by remotely connecting to PostgreSQL. Therefore, file system-related checks are not contained in this profile. Show Profile XML
Level 1 - PostgreSQL on Linux	Items in this profile apply to PostgreSQL 14 running on Linux and intend to: • be practical and prudent; • provide a clear security benefit; and • not inhibit the utility of the technology beyond acceptable means. Show Profile XML

Assessment Results

☐ Display Only Essential Hygiene (CIS Critical Security Controls V8- IG-1) ☐ Display Only Failures

More

w	Benchmark Item	Result
1 Installation and Patches		
	1.1 Ensure packages are obtained from authorized repositories	Manual
	1.2 Install only required packages	Manual
1.0	1.3 Ensure systemd Service Files Are Enabled	Fail

2.3 Disable PostgreSQL Command History

Manual

Description:

On Linux/UNIX, the PostgreSQL client logs most interactive statements to a history file. The default PostgreSQL history file is named `.psql_history` in the user's home directory.

The PostgreSQL command history should be disabled.

Rationale:

Disabling the PostgreSQL command history reduces the probability of exposing sensitive information, such as passwords, encryption keys, or sensitive data.

Remediation:

For each OS user on the PostgreSQL server, perform the following steps to implement this setting:

1. Remove `.psql_history` if it exists.
   ```
   rm -f ~<user>/.psql_history || true
   ```
2. Use either of the techniques below to prevent it from being created again:
   1. Set the `HISTFILE` variable to `/dev/null` in `~<user>/.psqlrc`
      ```
      cat << EOF >> ~<user>/.psqlrc \set HISTFILE /dev/null EOF
      ```
   2. Create `~<user>/.psql_history` as a symbolic to `/dev/null` .
      ```
      ln -s /dev/null $HOME/.psql_history
      ```
3. Set the `PSQL_HISTORY` variable for all users:
   ```
   sudo echo 'PSQL_HISTORY=/dev/null' >> /etc/environment
   ```

Show Rule Result XML

References:

- **URL:** https://www.postgresql.org/docs/current/app-psql.html#APP-PSQL-VARIABLES-HISTFILE

CIS Critical Security Controls V8.0:

- **Control 3: Data Protection:** -- More
  >

Back to Summary

MICHELIN

CIS WorkBench / Dashboard

workbench.cisecurity.org/dashboard

Redémarrer pour mettre à jour

Intranet France - Ho... | Sharepoint DAP D1... | InTouch, m&moi, é... | <developers/>_ dev... | <Documentation/>... | DBA - GitLab | JIRA | SNOW | Page d'accueil - GT... | CIS | EasyPPM | Rimini | Grafana Michelin D1 | EDB Home | Tous les favoris

CIS WorkBench
Member

Communities | Benchmarks | Tickets | Downloads | ? Support Center | alexymace

Welcome Alexy Mace

Get Started

Begin exploring **Communities**

Find out more about **CIS Controls**

Quick Links

Published **Benchmarks** List

CIS Controls Resources

Join A Community Today!

My Tickets

No Tickets

Community Activity

Benchmarks Activity

No Recent Activity.

Feedback

https://workbench.cisecurity.org/benchmarks

scan CIS PostgreSQL - (Nov 25, 2025): Vulnerability Summary

Vulnerability Summary

New | Mitigated | All | Switch to Full Cumulati

Vulnerabilities | Web App Scanning | Queries | Events | Mobile

107 Result(s) | Go to Vulnerability Detail | Export | Save | More

1 to 50 of 107 | Page 1 of 3

Plugin ID	Name	Family	Severity	VPR	EPSS (...	Total	Host Total
1001683	3.1.4 Ensure the log file destination directory is set correctly	N/A	HIGH			84	84
1001684	3.1.5 Ensure the filename pattern for log files is set correctly	N/A	HIGH			84	84
1001773	CIS_PostgreSQL_14_v 1.2.0_L1_DB.audit from CIS PostgreSQL 14 Bench...	N/A	MEDIUM			87	87
1001786	CIS_PostgreSQL_15_v1.1.0_L1_Database.audit from CIS PostgreSQL 15 B...	N/A	MEDIUM			87	87
1001790	CIS_PostgreSQL_16_v1.0.0_L1_Database.audit from CIS PostgreSQL 16 B...	N/A	MEDIUM			87	87
1001792	CIS_PostgreSQL_13_v1.2.0_L1_DB.audit from CIS PostgreSQL 13 Benchm...	N/A	MEDIUM			87	87
1001681	3.1.2 Ensure the log destinations are set correctly	N/A	INFO			84	84
1001682	3.1.3 Ensure the logging collector is enabled	N/A	INFO			84	84
1001686	3.1.7 Ensure 'log_truncate_on_rotation' is enabled	N/A	INFO			84	84
1001687	3.1.8 Ensure the maximum log file lifetime is set correctly	N/A	INFO			84	84

MICHELIN

scan CIS PostgreSQL - (Nov 25, 2025): Vulnerability Summary > Vulnerability List

Vulnerability List

New | Mitigated | All | Switch to Full Cumulative

Vulnerabilities | Web App Scanning | Queries | Events | Mobile

84 Result(s) | Go to Vulnerability Detail | Export | Save | More

1 to 50 of 84 | Page 1 of 2

Plugin ID	Plugin Name	Family	Severity	VPR	EPS...	IP Address	NetBIOS	DNS	MAC Address	Port	Protocol	Repositor
1001685	3.1.6 Ensure the lo...	N/A	INFO			[redacted]		[redacted]	[redacted]	0	TCP	Individual S
1001685	3.1.6 Ensure the lo...	N/A	INFO			[redacted]		[redacted]	[redacted]	0	TCP	Individual S
1001685	3.1.6 Ensure the lo...	N/A	HIGH			[redacted]		[redacted]	[redacted]	0	TCP	Individual S
1001685	3.1.6 Ensure the lo...	N/A	INFO			[redacted]		[redacted]	[redacted]	0	TCP	Individual S
1001685	3.1.6 Ensure the lo...	N/A	INFO			[redacted]		[redacted]	[redacted]	0	TCP	Individual S
1001685	3.1.6 Ensure the lo...	N/A	INFO			[redacted]		[redacted]	[redacted]	0	TCP	Individual S
1001685	3.1.6 Ensure the lo...	N/A	HIGH			[redacted]		[redacted]	[redacted]	0	TCP	Individual S
1001685	3.1.6 Ensure the lo...	N/A	INFO			[redacted]		[redacted]	[redacted]	0	TCP	Individual S

Vulnerability Detail List

Vulnerabilities | Web App Scanning | Queries | Events | Mobile

3.1.9 Ensure the maximum log file size is set correctly (1001688)

VULNERABILITY HIGH

automatic log file rotation when files become too large, which could put log data at increased risk of loss (unless age-based rotation is configured).

See Also

LINKS:
cisecurity.org

Policy Value

SQL_POLICY
sql_request: show log_rotation_size
sql_expect: STRING - 1GB

Output

RESULT: FAILED

OUTPUT:

```
5445/no_name:
  ["0"]
```

Copy

Assessment Configuration

NESSUS WEB TESTS: N/A
THOROUGH TESTS: N/A
SCAN ACCURACY: N/A

Reference Information

800-53: AU-4
800-53R5: AU-4
CSCV7: 6.4
CSCV8: 8.3
CSF: PR.DS-4
CSF: PR.PT-1
GDPR: 32.1.b
HIPAA: 164.306(a)(1)
HIPAA: 164.312(b)
ITSG-33: AU-4
LEVEL: 1A
NESA: T3.3.1
NESA: T3.6.2

MICHELIN

ANALYSE DES RÉSULTATS

Les solutions de Benchmark permettent donc de faire une première analyse du score de sécurité

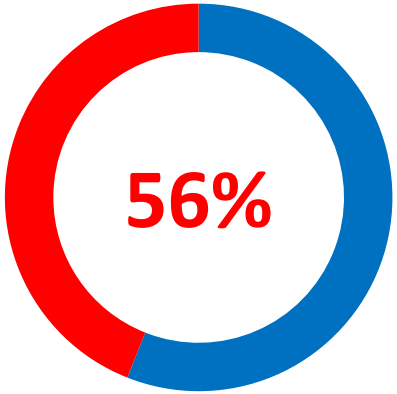
Cependant, dans le cas de PostgreSQL, une analyse manuelle est nécessaire pour les recommandations n'étant pas vérifiées automatiquement

Cette analyse manuelle permettra donc d'obtenir le score exact de sécurité de vos bases de données

MICHELIN

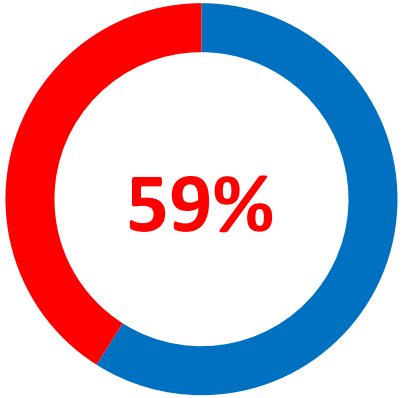
RETOUR À NOTRE EXEMPLE

Score de sécurité donné par le benchmark



33 recommandations

Score de sécurité final incluant les recommandations à analyse manuelle



68 recommandations

ÉVALUATION DES RECOMMANDATIONS

Identifier les recommandations non pertinentes à mettre en place (ex. Contraintes métier, architecture spécifique)

Identifier leurs impacts sur les users et l'accès aux données

Documenter et faire des éventuelles demandes de dérogation au service sécurité

MICHELIN

PRIORISATION

Pourquoi prioriser et mettre en place les recommandations en plusieurs étapes?

- *Augmenter plus rapidement le score de sécurité*
- *Faciliter l'analyse si des erreurs apparaissent*
- Permet de diviser les tâches entre plusieurs personnes pour un meilleur partage des compétences

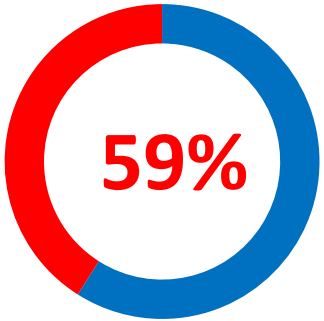
Comment a été réalisé la priorisation?

- *Répondre en priorité aux MGSR (Michelin Global Security Rules)*
- *Mettre en place les recommandations faciles et rapides à mettre en place*
- *Travailler sur les recommandations plus complexes ou incluant des plugins*

MICHELIN

SCORE CIBLE DE NOTRE EXEMPLE

Score actuel

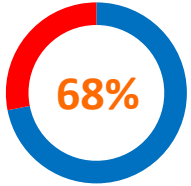


40/68 recommandations PASS

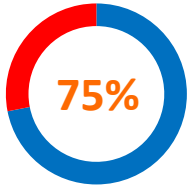
Sur les 28 recommandations fail

19 ont été identifiées comme pouvant être mises en place

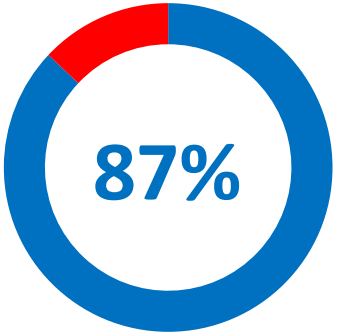
Etape 1:
6 recommandations



Etape 2:
5 recommandations



Score final



59/68 recommandations PASS

MISE EN OEUVRE SUR L'ENSEMBLE DES BASES

Pour chaque palier de recommandations, 5 étapes:

1. Mettre à jour les scripts de déploiement de nouvelles bases de données
2. Créer un script (yml) de mise à jour des paramètres sur les bases de données déjà en place
3. Lancer ce script sur les bases de pré prod
4. Vérifier qu'aucun problème ne soit détecté
5. Puis le lancer sur les bases de production

MICHELIN

SUR LE LONG TERME

- 1 version majeure par an
- Nouvelles recommandations CIS régulières
- Mettre en place des tests de compliance mensuels (Tenable)

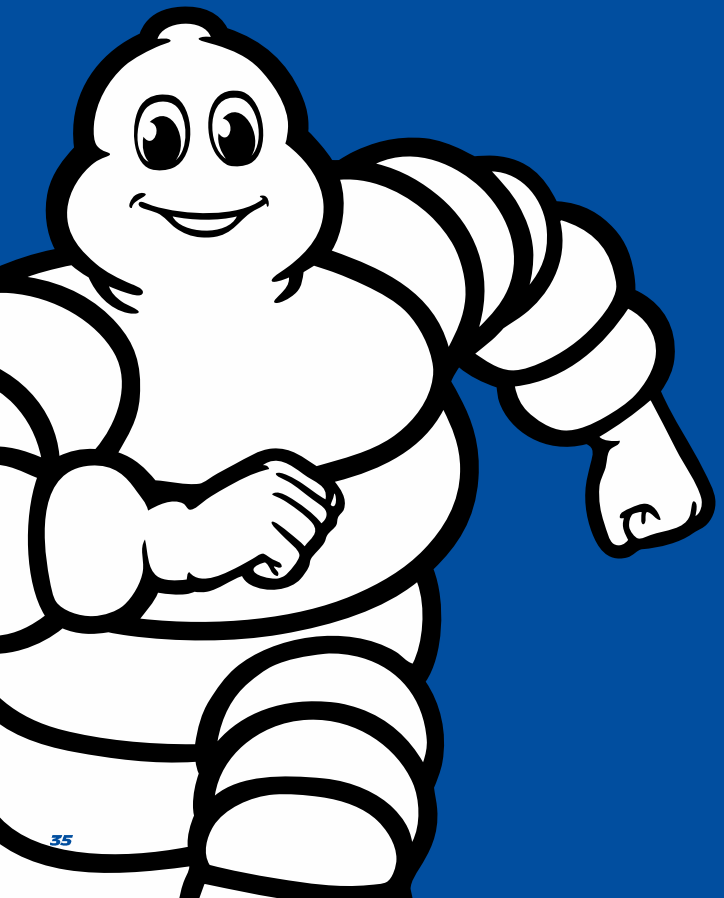
POUR CONCLURE

POUR CONCLURE

CIS Center for Internet Security®

- Les CIS sont un bon moyen pour améliorer la sécurité des bases de données PostgreSQL
- Leurs nombreuses recommandations offrent un large spectre d'ameliorations
- Les CIS peuvent être utilisé pour améliorer la sécurité d'autres solutions (serveurs, réseau, d'autres solutions de bases de données)

MICHELIN

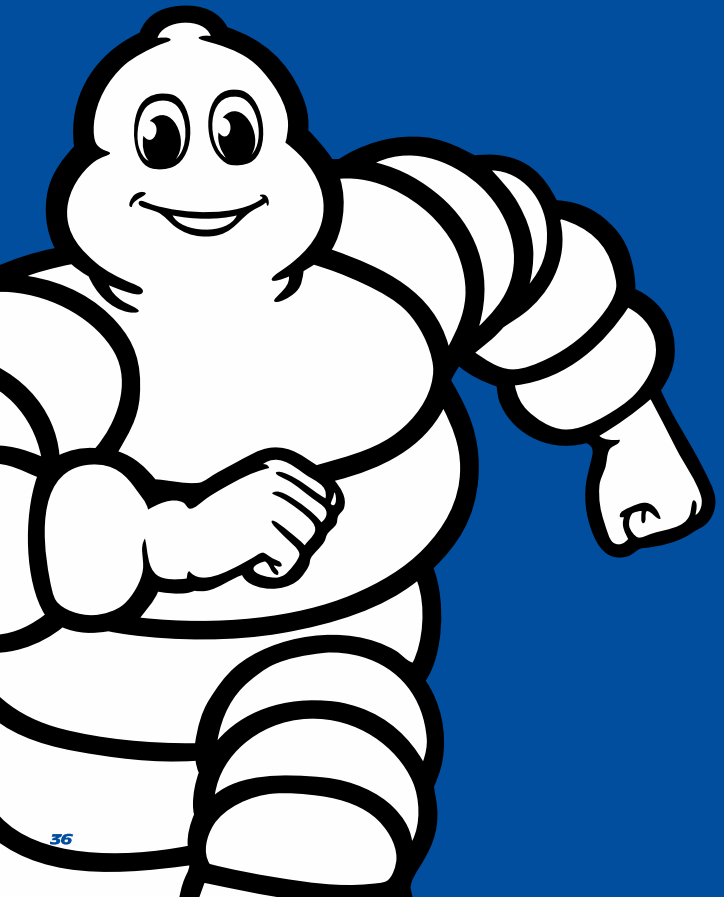


MERCI DE VOTRE ATTENTION !

ALEXY MACE

JEAN-LUC BENHAIM

MICHELIN



MOTION FOR LIFE

MICHELIN