RAPPORT DE PRÉPARATION CYBER ESSENTIALS

Example GmbH

PÉRIODE	DOMAINES	HÔTES	ÉTABLI LE
23/06/2026 – 21/09/2026	1	8	14/10/2026

Ce rapport rattache les constats de Example GmbH visibles depuis l'extérieur aux cinq mesures techniques de Cyber Essentials, le dispositif de certification du NCSC britannique (exigences v3.3, questionnaire « Danzell », en vigueur depuis le 27 avril 2026). Il montre où une action est déjà visible depuis l'extérieur et ce qu'il vous reste à prouver en interne. veyrisk ne certifie pas.

1. Vue d'ensemble

4 constats ouverts entraîneraient probablement un échec. Corrigez-les avant de remettre votre auto-évaluation.

MESURE	ÉTAT	CONSTATS OUVERTS	ÉCHEC PROBABLE
Pare-feu	CONSTATS OUVERTS	3	2
Configuration sécurisée	CONSTATS OUVERTS	5	0
Gestion des mises à jour de sécurité	CONSTATS OUVERTS	1	1
Contrôle d'accès des utilisateurs	CONSTATS OUVERTS	1	1
Protection contre les logiciels malveillants	NON ÉVALUABLE DEPUIS L'EXTÉRIEUR	0	0

2. Pare-feu

CONSTATS OUVERTS

Ce que veyrisk contrôle depuis l'extérieur

Seuls les services nécessaires doivent être accessibles depuis Internet. veyrisk contrôle les ports ouverts (uniquement avec preuve de propriété), les interfaces d'administration accessibles publiquement ainsi que les systèmes de développement et de test.

GRAVITÉ	CONSTAT	OUVERT DEPUIS (JOURS)	REMARQUE
ÉLEVÉ	vpn.example.com RDP accessible depuis Internet (port 3389)	38	ÉLEVÉ OU CRITIQUE ET OUVERT DEPUIS PLUS DE 14 JOURS
ÉLEVÉ	shop.example.com Interface d'administration accessible publiquement (phpMyAdmin)	61	ÉLEVÉ OU CRITIQUE ET OUVERT DEPUIS PLUS DE 14 JOURS
MOYEN	dev.example.com Système de développement ou de test accessible publiquement	61	

À prouver en interne

- Un pare-feu à chaque frontière avec Internet, mot de passe par défaut modifié
- Chaque règle entrante documentée et justifiée, règles devenues inutiles supprimées
- Un pare-feu logiciel sur les appareils utilisés sur des réseaux non maîtrisés, comme le Wi-Fi public

3. Configuration sécurisée

CONSTATS OUVERTS

Ce que veyrisk contrôle depuis l'extérieur

Appareils et services sont durcis : pas de logiciels inutiles, pas de comptes par défaut, des réglages sûrs. veyrisk contrôle les certificats, TLS, HTTPS, les en-têtes de sécurité et la divulgation de versions, ainsi que les constats de configuration issus des analyses d'applications web et du cloud.

GRAVITÉ	CONSTAT	OUVERT DEPUIS (JOURS)	REMARQUE
MOYEN	mail.example.com Le certificat TLS expire dans 9 jours	3	
MOYEN	shop.example.com En-tête Strict-Transport-Security absent	90	
FAIBLE	www.example.com Version du logiciel divulguée dans l'en-tête Server (Apache/2.4.49)	45	
FAIBLE	www.example.com En-tête Content-Security-Policy absent	90	

FAIBLE	portal.example.com En-tête X-Content-Type-Options absent	90

À prouver en interne

- Logiciels, services et comptes utilisateurs inutiles supprimés ou désactivés
- Mots de passe par défaut modifiés, exécution automatique désactivée
- Verrouillage par code PIN, mot de passe ou biométrie sur tous les appareils

4. Gestion des mises à jour de sécurité

CONSTATS OUVERTS

Ce que veyrisk contrôle depuis l'extérieur

Tous les logiciels sont sous licence et encore pris en charge par l'éditeur. Les mises à jour critiques et à haut risque doivent être installées dans les 14 jours suivant leur publication. veyrisk s'appuie pour cela sur les constats d'Advanced Vulnerability Detection et sur les constats d'applications web associés à une CVE.

GRAVITÉ	CONSTAT	OUVERT DEPUIS (JOURS)	REMARQUE
ÉLEVÉ	vpn.example.com OpenSSH 'regreSSHion' Remote Code Execution Vulnerability (22/tcp)	26	ÉLEVÉ OU CRITIQUE ET OUVERT DEPUIS PLUS DE 14 JOURS

À prouver en interne

- Inventaire de tous les appareils du périmètre avec système d'exploitation et version
- Uniquement des systèmes d'exploitation et applications pris en charge, les autres supprimés ou isolés
- Mises à jour automatiques activées si possible, sinon preuve d'installation sous 14 jours

5. Contrôle d'accès des utilisateurs

CONSTATS OUVERTS

Ce que veyrisk contrôle depuis l'extérieur

Les comptes ne sont créés qu'en cas de besoin et les droits d'administrateur s'exercent via des comptes distincts. La MFA est obligatoire sur tous les services cloud qui la proposent ; sans elle, l'évaluation échoue automatiquement. Les passkeys comptent comme une connexion sans mot de passe. veyrisk ne le voit que dans les comptes cloud et Microsoft 365 connectés.

GRAVITÉ	CONSTAT	OUVERT DEPUIS (JOURS)	REMARQUE

ÉLEVÉ	Microsoft 365 (example.com) Ensure multifactor authentication is enabled for all users	9	MFA ABSENTE : ÉCHEC AUTOMATIQUE

À prouver en interne

- MFA pour tous les utilisateurs sur chaque service cloud qui la propose
- Comptes administrateur distincts, non utilisés pour la messagerie ni la navigation
- Un processus défini pour créer et supprimer les comptes, avec une revue régulière des droits
- Règles de mots de passe ou connexion sans mot de passe par passkeys, protection contre les attaques par force brute

6. Protection contre les logiciels malveillants

NON ÉVALUABLE DEPUIS L'EXTÉRIEUR

Ce que veyrisk contrôle depuis l'extérieur

Une protection contre les logiciels malveillants fonctionne sur tous les appareils du périmètre. Cela ne se contrôle pas depuis l'extérieur.

La protection contre les logiciels malveillants ne se contrôle pas depuis l'extérieur.

À prouver en interne

- Antivirus avec signatures à jour sur tous les appareils, ou liste d'applications autorisées
- Analyse des fichiers à l'accès et protection contre les sites web malveillants

7. Remarques et limites

Ce rapport est un contrôle de préparation depuis l'extérieur et non une certification. veyrisk ne certifie pas. Cyber Essentials et Cyber Essentials Plus sont délivrés uniquement par des organismes de certification agréés par l'IASME ; Cyber Essentials Plus ajoute des tests techniques. Le certificat est valable 12 mois.

Le périmètre couvre tous les appareils connectés à Internet et tous les services cloud. veyrisk ne voit que les systèmes accessibles publiquement de vos domaines et les comptes cloud connectés. La protection contre les logiciels malveillants et l'essentiel du contrôle d'accès ne se contrôlent pas depuis l'extérieur.

Le rattachement des constats aux mesures est une appréciation de veyrisk. Les constats sur l'authentification des e-mails (SPF, DMARC, MTA-STS) ne relèvent d'aucune des cinq mesures et n'apparaissent pas ici. Font foi les exigences du NCSC et l'appréciation de votre organisme de certification.

VEYRISK · NEONOTU GMBH

Edelsbergstraße 8, 80686 München · +49 89 2000 7975 0 · contact@veyrisk.com