

■ RAPPORT · SURFACE D'ATTAQUE EXTERNE

example.com

DATE DE L'ANALYSE 21/09/2026 08:00	PÉRIMÈTRE Passive et active (avec vérification des ports) + OpenVAS	HÔTES VÉRIFIÉS 8	SOURCES crt.sh, certspotter
---------------------------------------	--	---------------------	--------------------------------

SCORE D'EXPOSITION

36 / 100



Priorité moyenne de tous les constats, de 0 à 100. Plus il est bas, mieux c'est.

CONSTATS: 10

0 CRITIQUE	3 ÉLEVÉE	3 MOYENNE	4 FAIBLE
---------------	-------------	--------------	-------------

L'essentiel en bref

Traitez ces constats en priorité. Ils associent une gravité élevée à l'importance du système concerné.

PRIO.	GRAVITÉ	CONSTAT ET RECOMMANDATION
61	ÉLEVÉE	vpn.example.com OpenSSH 'regreSSHion' Remote Code Execution Vulnerability (22/tcp) → Update OpenSSH to version 9.8p1 or later.
56	ÉLEVÉE	vpn.example.com RDP accessible depuis Internet (port 3389) → Fermez le port dans le pare-feu ou limitez-le à des adresses IP connues.
56	ÉLEVÉE	shop.example.com Interface d'administration accessible publiquement (phpMyAdmin) → Rendez-la accessible uniquement via VPN ou une liste d'adresses IP autorisées.
34	MOYENNE	dev.example.com Système de développement ou de test accessible publiquement → Protégez-le par une authentification, un VPN ou une liste d'adresses IP autorisées, et arrêtez les systèmes devenus inutiles.
34	MOYENNE	mail.example.com Le certificat TLS expire dans 9 jours → Renouvelez le certificat et vérifiez que le renouvellement automatique fonctionne.

Tous les constats par hôte

example.com

PRIO.	GRAVITÉ	CONSTAT ET RECOMMANDATION
24	FAIBLE	La politique DMARC est p=none, les e-mails usurpés ne sont pas rejetés → Après analyse des rapports, relevez la politique à p=quarantine ou p=reject.

www.example.com

PRIO.	GRAVITÉ	CONSTAT ET RECOMMANDATION
24	FAIBLE	Version du logiciel divulguée dans l'en-tête Server (Apache/2.4.49) → Désactivez l'affichage de la version dans le serveur web (p. ex. server_tokens off, ServerTokens Prod).
20	FAIBLE	En-tête Content-Security-Policy absent → Définissez une Content-Security-Policy qui n'autorise que les sources nécessaires.

shop.example.com

PRIO.	GRAVITÉ	CONSTAT ET RECOMMANDATION
56	ÉLEVÉE	Interface d'administration accessible publiquement (phpMyAdmin) → Rendez-la accessible uniquement via VPN ou une liste d'adresses IP autorisées.
32	MOYENNE	En-tête Strict-Transport-Security absent → Définissez Strict-Transport-Security: max-age=31536000; includeSubDomains.

mail.example.com

PRIO.	GRAVITÉ	CONSTAT ET RECOMMANDATION
34	MOYENNE	Le certificat TLS expire dans 9 jours → Renouvelez le certificat et vérifiez que le renouvellement automatique fonctionne.

vpn.example.com

PRIO.	GRAVITÉ	CONSTAT ET RECOMMANDATION
61	ÉLEVÉE	OpenSSH 'regreSSHion' Remote Code Execution Vulnerability (22/tcp) → Update OpenSSH to version 9.8p1 or later.
56	ÉLEVÉE	RDP accessible depuis Internet (port 3389) → Fermez le port dans le pare-feu ou limitez-le à des adresses IP connues.

dev.example.com

PRIO.	GRAVITÉ	CONSTAT ET RECOMMANDATION
34	MOYENNE	Système de développement ou de test accessible publiquement → Protégez-le par une authentification, un VPN ou une liste d'adresses IP autorisées, et arrêtez les systèmes devenus inutiles.

portal.example.com

PRIO.	GRAVITÉ	CONSTAT ET RECOMMANDATION
17	FAIBLE	En-tête X-Content-Type-Options absent → Définissez X-Content-Type-Options: nosniff.

Aucun constat

cdn.example.com

Méthode et limites

Les sous-domaines proviennent des journaux publics de certificats (Certificate Transparency). Seuls les hôtes résolus par DNS ont été vérifiés.

Pour chaque hôte, nous avons vérifié le certificat TLS, la redirection de HTTP vers HTTPS, les en-têtes de sécurité de la page d'accueil et les interfaces d'administration identifiables, ainsi que SPF et DMARC pour le domaine principal.

Une analyse passive ne vérifie pas les ports ouverts et n'attaque pas les applications. Elle montre ce qui est visible de l'extérieur sans identifiants.

Ce rapport est un instantané au moment indiqué. La priorité est une évaluation et ne remplace pas un test d'intrusion.

En complément, une analyse active des vulnérabilités des adresses publiques a été réalisée avec OpenVAS (Greenbone), sur la base de la propriété vérifiée du domaine. Seuls les constats présentant une qualité de détection d'au moins 70 % ont été retenus.

Prochaines étapes

Nous serons heureux de vous présenter ce rapport et de vous montrer comment veyrisk surveille votre surface d'attaque en continu, au lieu d'un simple coup d'œil ponctuel.

CONTACT

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