TECHATELIER / INFRACHECK

Audit report

Infrastructure and public exposure

example.com

Passive assessment based on public data - not a substitute for an intrusive security audit.

Analysis generated on 2026-07-23 12:00

OVERALL SCORE	GRADE	MATURITY	ACTIONS
82/100	B	Level 4 - Advanced	3

Overview

Control results by category

CATEGORY	SCORE	PASSED	TO FIX
DNS	92/100	2	1
TLS	90/100	2	0
HTTP	72/100	1	1
Email	74/100	2	1

DNS

Category score: 92/100

STATUS	CHECK	OBSERVATION
COMPLIANT	IPv4 resolution	Public IPv4 address detected.
COMPLIANT	DNS servers	Two authoritative name servers respond.
TO FIX	DNSSEC	No DNSSEC chain of trust detected.

TLS

Category score: 90/100

STATUS	CHECK	OBSERVATION
COMPLIANT	HTTPS certificate	Valid certificate with a complete chain.

STATUS	CHECK	OBSERVATION
COMPLIANT	**Modern protocols**	TLS 1.2 and TLS 1.3 are available.

HTTP

Category score: 72/100

STATUS	CHECK	OBSERVATION
COMPLIANT	**Availability**	The website responds correctly over HTTPS.
TO FIX	**Content-Security-Policy**	The CSP header is missing from the response.

Email

Category score: 74/100

STATUS	CHECK	OBSERVATION
COMPLIANT	**SPF**	A valid SPF policy is published.
COMPLIANT	**DMARC**	A DMARC record is present.
TO FIX	**DMARC policy**	The p=none policy does not yet protect the domain.

Priority action plan

Recommended fixes, ranked by priority

PRIORITY	ACTION	IMPACT AND RECOMMENDATION
HIGH	**Add a CSP policy**	Impact: A CSP limits the exploitation of content injected into pages. Recommendation: Deploy a restrictive policy, then adjust it based on reports.
MEDIUM	**Enable DNSSEC**	Impact: DNSSEC reduces the risk of forged DNS responses. Recommendation: Enable DNSSEC through the domain registrar.
MEDIUM	**Strengthen DMARC**	Impact: The p=none policy observes messages without blocking them. Recommendation: Gradually move to quarantine and then reject after reviewing reports.