Dr.Who

Evidence Pack

example.com

Scanned 2026-05-11T12:00:00.000Z

Signing key: drwhome-evp-v1

what this is not

the Evidence Pack is supporting technical evidence for public-facing domain controls. it is not a SOC 2 audit report and does not replace an auditor; it gives them less to chase. it is not a penetration test, not a risk register, and not a substitute for compliance tooling like Vanta, Drata, or SecureFrame — those tools manage the audit programme; the pack documents the public domain surface they reference.

Demonstration artifact — synthetic findings, signed for verification only.

Built by Hikmah Technologies
hikmahtechnologies.com

Executive Summary

Scanned 2 host(s); recorded 35 finding(s).

D

Multiple findings need attention

Aggregate grade across 15 checks. Auditors typically flag any High-severity finding.

PASS	WARN	FAIL
0	9	6

WHAT AN AUDITOR WOULD FLAG FIRST

HIGH **SPF**

No SPF record published — sender authentication absent

SOC 2 CC6.7 · ISO 27001 A.8.20 · NIST SC-8

HIGH **TLS certificate**

Certificate expired 14 days ago

SOC 2 CC6.1 · ISO 27001 A.8.24 · NIST SC-8(1)

HIGH **Certificate Transparency**

Unexpected CT log entry from unfamiliar issuer

SOC 2 CC7.2 · ISO 27001 A.8.16 · NIST SI-4

CRITICAL · 2 | HIGH · 4 | MEDIUM · 6 | LOW · 8 | INFO · 15

Severity	Count
Critical	2
High	4
Medium	6
Low	8
Info	15

Critical 2 findings

spf · example.com

No SPF record published — sender authentication absent

Pain: does this domain publish an SPF record limiting authorised senders?

SOC 2 CC6.7 | ISO 27001 A.8.20 | NIST SC-8

- Publish an SPF TXT record covering all senders

tls · example.com

Certificate expired 14 days ago

Pain: is data in transit protected by a valid, current TLS certificate?

SOC 2 CC6.1 | ISO 27001 A.8.24 | NIST SC-8(1)

- Renew the TLS certificate immediately

High

4 findings

ct_log · example.com

Unexpected CT log entry from unfamiliar issuer

Pain: which subdomains have certificates issued in CT logs for this root?

SOC 2 CC7.2 | ISO 27001 A.8.16 | NIST SI-4

dkim · example.com

DKIM selector default not found

Pain: are outgoing emails DKIM-signed under a published selector?

SOC 2 CC6.7 | ISO 27001 A.8.24 | NIST SC-8

- Publish a DKIM key for the default selector

dmarc · example.com

DMARC policy is p=none (monitor-only)

Pain: does this domain enforce a DMARC policy (quarantine or reject)?

SOC 2 CC6.7 | ISO 27001 A.5.14 | NIST SC-8

- Tighten DMARC policy to quarantine then reject after monitoring

headers · example.com

Strict-Transport-Security header missing

Pain: are HSTS, CSP, X-Frame-Options, and related headers configured?

SOC 2 CC6.6 | ISO 27001 A.8.23 | NIST SC-7(8)

- Add HSTS header with max-age >= 31536000

Medium 6 findings

cors · example.com
Access-Control-Allow-Origin reflects arbitrary origin

Pain: are cross-origin policies appropriately restrictive at this origin?

SOC 2 CC6.6 | ISO 27001 A.8.23 | NIST AC-4

dnssec · example.com
DNSSEC NS records exist but no DS record at parent zone

Pain: is DNSSEC signing enabled for this zone?

SOC 2 CC6.6 | ISO 27001 A.8.20 | NIST SC-20

mta_sts · example.com
MTA-STS policy mode is `testing`, not `enforce`

Pain: does this domain enforce MTA-STS to prevent SMTP downgrade attacks?

SOC 2 CC6.7 | ISO 27001 A.8.24 | NIST SC-8

redirects · example.com
HTTP does not redirect to HTTPS

Pain: does the public site redirect HTTP to HTTPS without dropping the user?

SOC 2 CC6.6 | ISO 27001 A.8.23 | NIST SC-7

tlsrpt · example.com
TLSRPT record present but rua URI is unreachable

Pain: does this domain receive TLS-RPT reports for SMTP failures?

SOC 2 CC7.2 | ISO 27001 A.8.16 | NIST AU-6

whois · example.com
Registrant info is private but expiry in 28 days

Pain: who owns this domain and when does the registration expire?

SOC 2 CC2.3 | ISO 27001 A.5.20 | NIST PE-2

Low — 8 findings

dns · example.com
AAAA record absent (IPv6 unreachable)

Pain: are authoritative DNS records published correctly for this domain?

SOC 2 CC6.6 | ISO 27001 A.8.20 | NIST SC-20

dns · example.com
TXT record contains plaintext API key fragment (case-insensitive 'api')

Pain: are authoritative DNS records published correctly for this domain?

SOC 2 CC6.6 | ISO 27001 A.8.20 | NIST SC-20

headers · example.com
Content-Security-Policy header missing

Pain: are HSTS, CSP, X-Frame-Options, and related headers configured?

SOC 2 CC6.6 | ISO 27001 A.8.23 | NIST SC-7(8)

headers · example.com
X-Content-Type-Options header missing

Pain: are HSTS, CSP, X-Frame-Options, and related headers configured?

SOC 2 CC6.6 | ISO 27001 A.8.23 | NIST SC-7(8)

headers · example.com
Referrer-Policy header missing

Pain: are HSTS, CSP, X-Frame-Options, and related headers configured?

SOC 2 CC6.6 | ISO 27001 A.8.23 | NIST SC-7(8)

mx · example.com
MX backup priority value is below 10 (non-standard)

Pain: which mail servers are authoritative for receiving email at this domain?

SOC 2 CC6.7 | ISO 27001 A.8.21 | NIST SC-8

redirects · example.com
Final redirect target uses HTTP/1.1 not HTTP/2

Pain: does the public site redirect HTTP to HTTPS without dropping the user?

SOC 2 CC6.6 | ISO 27001 A.8.23 | NIST SC-7

web-surface · example.com

robots.txt exposes /admin path

Pain: what robots.txt, sitemap, and meta the domain advertises publicly.

SOC 2 CC6.6 | ISO 27001 A.8.9 | NIST CM-7

Info

15 findings

Detailed info findings are listed in Appendix B.

cors	1
ct_log	1
dkim	1
dmarc	1
dns	2
headers	2
mx	1
redirects	1
spf	1
tls	2
web-surface	1
whois	1

Appendix A — Framework Mapping

SOC 2	ISO 27001	NIST	Check	Observed
CC6.7	A.8.20	SC-8	spf	critical
CC6.1	A.8.24	SC-8(1)	tls	critical
CC7.2	A.8.16	SI-4	ct_log	high
CC6.7	A.8.24	SC-8	dkim	high
CC6.7	A.5.14	SC-8	dmarc	high
CC6.6	A.8.23	SC-7(8)	headers	high
CC6.6	A.8.23	AC-4	cors	medium
CC6.6	A.8.20	SC-20	dnssec	medium
CC6.7	A.8.24	SC-8	mta_sts	medium
CC6.6	A.8.23	SC-7	redirects	medium
CC7.2	A.8.16	AU-6	tlsrpt	medium
CC2.3	A.5.20	PE-2	whois	medium
CC6.6	A.8.20	SC-20	dns	low
CC6.7	A.8.21	SC-8	mx	low
CC6.6	A.8.9	CM-7	web-surface	low

Appendix B — Per-Check Raw Data

spf

host: example.com severity: critical

{"records":[]}

host: example.com severity: info

{"exists":true}

tls

host: example.com severity: critical

{"notAfter":"2026-04-27T00:00:00Z"}

host: example.com severity: info

{"issuer":"DigiCert TLS RSA SHA256 2020 CA1","notAfter":"2026-12-31T00:00:00Z"}

host: www.example.com severity: info

{"issuer":"DigiCert TLS RSA SHA256 2020 CA1"}

ct_log

host: example.com severity: high

{"issuers":["E-Sign Sample CA"]}

host: example.com severity: info

{"entries":8}

dkim

host: example.com severity: high

{"selectorsChecked":["default"]}

host: example.com severity: info

{"selectorsChecked":["default","google","mail"]}

dmarc

host: example.com severity: high

{"policy":"none"}

host: example.com severity: info

{"policy":"none","rua":"mailto:dmarc@example.com"}

headers

host: example.com severity: high

{"hsts":null}

host: example.com severity: low

{"csp":null}

host: example.com severity: low

{"xcto":null}

host: example.com severity: low

{"referrerPolicy":null}

host: example.com severity: info

{"hsts":"max-age=63072000; includeSubDomains; preload"}

host: www.example.com severity: info

{"hsts":null}

cors

host: example.com severity: medium

{"reflects":true}

host: example.com severity: info

{"preflight":{"acao":"https://example.com"}}

dnssec

host: example.com severity: medium

{"ds":null}

mta_sts

host: example.com severity: medium

{"mode":"testing"}

redirects

host: example.com severity: medium

{"http":200,"https":200}

host: example.com severity: low

{"protocol":"HTTP/1.1"}

host: example.com severity: info

{"chain":["http://example.com","https://example.com/"]}

tlsrpt

host: example.com severity: medium

{"rua":"mailto:tlsrpt@example.com"}

whois

host: example.com severity: medium

{"expiresIn":28}

host: example.com severity: info

{"registrar":"ICANN Reserved"}

dns

host: example.com severity: low

{"aaaa":[]}

host: example.com severity: low

{"suspicious":["api=demo-***"]}

host: example.com severity: info

{"records":{"A":["93.184.216.34"],"NS":["a.iana-servers.net"]}}

host: www.example.com severity: info

{"records":{"A":["93.184.216.34"]}}

mx

host: example.com severity: low

{"backupPriority":5}

host: example.com severity: info

{"records":[]}

web-surface

host: example.com severity: low

{"sensitivePaths":["/admin"]}

host: example.com severity: info

{"robots":"User-agent: *\nDisallow: /admin\n"}