Prepared for

Sample Company

Prepared by EightScope · External website, DNS, email and infrastructure assessment

Security Report

sample-company.example

Company, domain and findings are anonymised demonstration data.

Demonstration · Anonymised sample data

01 · Executive summary

sample-company.example

In plain English

sample-company.example scored 86/100 (grade A) with 12 issue(s) to review. This is an external posture assessment, not a penetration test or compliance certification.

Completed	Scan type	Duration
13 Jul 2026, 10:51 UTC	Full	73s

Scan ID

`sample-00000000-0000-4000-8000-000000000001`

86 · **Grade A**

Strong external posture

External assessment score out of 100 (this scan only) · 12 host-level findings · 8 grouped issues · 51 Successful check instances

0	0	4	8	0
Critical	High	Medium	Low	Info

12 host-level findings · **8** grouped issues in detail · **51** Successful check instances

Assets - discovered: **13** · reachable: **13** · fully assessed: **11** · partially assessed: **1** · error: **1** · unassessed: **0**

TLS - attempted: **12** · completed: **11** · errors: **1** · unassessed: **1**

02 · Score explanation

How the external risk score was calculated for this scan.

Starting score: **100** · Points lost: **14** · Final: **86** (grade A)

Confirmed findings deduct full severity weight. Likely findings and legacy findings without a rated confidence deduct half (rounded down). Possible and inconclusive findings do not affect the score. Passed checks do not add points. They avoid deductions that would apply if the same check had failed.

Check	Severity	Confidence	Points	Host
Content Security Policy (CSP) missing	Medium	Confirmed	–3	2 hosts: elements.sample-company.example, app.sample-company.example
Clickjacking protection missing (X-Frame-Options / frame-ancestors)	Medium	Confirmed	–3	app.sample-company.example
Cookie Scope: sample_company_client_id	Medium	Confirmed	–3	sample-company.example
CAA record missing	Low	Confirmed	–1	sample-company.example
MIME sniffing protection missing	Low	Confirmed	–1	2 hosts: elements.sample-company.example, app.sample-company.example
Referrer-Policy not set	Low	Confirmed	–1	2 hosts: elements.sample-company.example, app.sample-company.example
Permissions-Policy not set	Low	Confirmed	–1	2 hosts: elements.sample-company.example, app.sample-company.example
MTA-STS (Email TLS)	Low	Confirmed	–1	_mta-sts.sample-company.example

Capped duplicate deductions

· Content Security Policy (CSP) missing on app.sample-company.example - Same check on another host; score uses the worst instance only

· MIME sniffing protection missing on app.sample-company.example - Same check on another host; score uses the worst instance only

· Referrer-Policy not set on app.sample-company.example - Same check on another host; score uses the worst instance only

· Permissions-Policy not set on app.sample-company.example - Same check on another host; score uses the worst instance only

Grade explanation

· Numeric score 86/100 falls in the 80-89 without grade ceilings band.

03 · Priority actions

Highest-impact fixes first. Full evidence and steps are on each finding page.

1. Clickjacking protection missing (X-Frame-Options / frame-ancestors) · Medium · Confirmed · Security / IT · Effort: Small

Why it matters

Your pages can be embedded in an iframe on another site. Attackers use this to overlay invisible frames and trick users into clicking actions they did not intend.

Hosts (1): app.sample-company.example

Timeframe: Fix within 30 days, sooner on admin or payment flows.

2. Content Security Policy (CSP) missing · Medium · Confirmed · Web / application team · Effort: Small

Why it matters

Your site sends no Content-Security-Policy header. Without CSP there is no browser-enforced resource allowlist to limit the impact of injected markup or scripts. CSP does not inve…

Hosts (2): elements.sample-company.example, app.sample-company.example

Timeframe: Plan within 30 days; not an emergency on its own.

3. Cookie scoped too broadly · Medium · Confirmed · Web / application team · Effort: Small

Why it matters

A cookie is set with a Domain attribute that covers the whole registrable domain, so every subdomain can receive it. A compromised subdomain could steal application or login-sessi…

Hosts (1): sample-company.example

Timeframe: Fix within 2 weeks for session and auth cookies.

4. MIME sniffing protection missing · Low · Confirmed · Security / IT · Effort: Small

Why it matters

Without X-Content-Type-Options: nosniff, browsers may guess content types and treat uploaded or mislabeled files as executable content.

Hosts (2): elements.sample-company.example, app.sample-company.example

Timeframe: Fix in the next maintenance window.

5. Referrer-Policy not set · Low · Confirmed · Security / IT · Effort: Small

Why it matters

No Referrer-Policy header is set, so referrer behaviour falls back to browser defaults. Modern browsers usually default to strict-origin-when-cross-origin, but an explicit header…

Hosts (2): elements.sample-company.example, app.sample-company.example

Timeframe: Fix within 60 days.

04 · Module status

What ran, what was excluded, and why. Full coverage detail is at the end of this report.

Module	Status	Assets checked	Reason
DNS and email authentication	Completed	-	-
TLS / certificates	Completed with gaps	11 completed, 1 error, 1 unassessed (of 12 attempted)	11 completed, 1 error, 1 unassessed
Port scan	Completed	-	-
HTTP security headers	Completed	13	-
Exposed files	Completed	-	-
Domain registration (WHOIS)	Completed	-	-
Directory listing	Completed	-	-
Cloud storage exposure	Completed	-	-
Cookie security	Completed	-	-
JavaScript libraries	Completed	-	-
WAF / CDN detection	Completed	-	-
Email security depth	Completed	-	-
Certificate Transparency	Completed	-	-
Email address harvest	Completed	-	-
JavaScript secrets	Completed	-	-
Lookalike domains	Completed	-	-
Login panel exposure	Completed	-	-
Web hygiene	Completed	-	-
Service banners	Completed	-	-

WordPress	Completed	-	-
Open redirects	Completed	-	-
API discovery	Completed	-	-
Rate limiting	Completed	-	-
CVE mapping	Completed	-	-
Reputation / Safe Browsing	Not assessed	-	Provider not configured for this scan
Website performance	Completed	-	-
Subdomain discovery	Completed	-	-

05 · Asset inventory

Hosts discovered during this scan. Unassessed hosts are marked clearly.

Hostname	Source	IPs	CDN	TLS	Headers	Assessment
sample-company.example	verified_domain	104.18.208.202 104.16.239.191	Yes	scanned	scanned	**Fully assessed** Cert: 2026-08-24T03:27:01+00:00
www.sample-company.example	dns_bruteforce	172.64.147.157 104.18.40.99	Yes	scanned	scanned	**Fully assessed** Cert: 2026-08-24T03:24:54+00:00
api.sample-company.example	dns_bruteforce	104.18.39.94, 172.64.148.162	Yes	scanned	scanned	**Fully assessed** Cert: 2026-08-23T13:04:55+00:00
app.sample-company.example	dns_bruteforce	104.18.17.100, 104.18.16.100	Yes	scanned	scanned	**Fully assessed** Cert: 2026-09-28T04:46:10+00:00
blog.sample-company.example	dns_bruteforce	104.16.239.191 104.18.208.202	Yes	scanned	scanned	**Fully assessed** Cert: 2026-08-23T11:01:40+00:00
careers. sample-company. example	dns_bruteforce	104.18.208.202 104.16.239.191	Yes	scanned	scanned	**Fully assessed** Cert: 2026-08-24T04:53:32+00:00
community. sample-company. example	dns_bruteforce	104.16.239.191 104.18.208.202	Yes	scanned	scanned	**Fully assessed** Cert: 2026-08-23T20:44:48+00:00
forum.sample-company.example	dns_bruteforce	52.217.90.27, 52.216.45.13, 16.15.199.10, 16.182.66.125	No	error	scanned	**Error** TLS check started but could not complete. Cert: None
intranet. sample-company. example	dns_bruteforce	104.16.239.191 104.18.208.202	Yes	scanned	scanned	**Fully assessed** Cert: 2026-08-26T08:31:36+00:00
s3.sample-company.example	dns_bruteforce	108.158.32.109 108.158.32.36, 108.158.32.99, 108.158.32.4	Yes	scanned	scanned	**Fully assessed** Cert: 2027-01-18T23:59:59+00:00
status. sample-company. example	dns_bruteforce	3.175.115.129, 3.175.115.46, 3.175.115.7, 3.175.115.39	Yes	scanned	scanned	**Fully assessed** Cert: 2026-09-12T13:22:45+00:00
support. sample-company. example	dns_bruteforce	104.16.239.191 104.18.208.202	Yes	scanned	scanned	**Fully assessed** Cert: 2026-08-24T03:29:37+00:00

elements. sample-company. example	finding_host, dns_bruteforce	104.18.208.202 104.16.239.191	Yes	unassessed	scanned	**Partially assessed** HTTPS was reachable and headers were assessed; this host was within the Full-scan TLS host limit, but TLS certificate capture was not recorded (coverage gap).; HTTPS reachable and headers assessed; host is within the Full-scan TLS limit of 20 non-apex hosts, but TLS certificate capture was not recorded for this host (coverage gap). Cert: None

06 · Website performance

External lab test via Google PageSpeed Insights (mobile). Not real visitor analytics. Separate from the cybersecurity score.

Overall (mobile)	**78/100** · needs improvement · Pages tested: 4 / discovered: 4 Selected up to 5 important pages using homepage links, sitemap paths.
Slowest page	`https://sample-company.example/services · score 69 · LCP 3800 ms`
Top improvements	1. Properly size images (~600 ms) 2. Reduce unused JavaScript (~510 ms) 3. Eliminate render-blocking resources (~280 ms)

Page	Type	Score	LCP	CLS
`https://sample-company.example/`	homepage	84	2600 ms	0.04
`https://sample-company.example/login`	login account	71	3200 ms	0.08
`https://sample-company.example/contact`	contact booking	88	2100 ms	0.02
`https://sample-company.example/services`	service product	69	3800 ms	0.11

07 · Detailed findings

8 grouped issues with evidence, context, and recommended fixes. Built from 12 host-level findings (same counts as the interactive sample).

How to read this section

Each issue starts on its own page. Navy blocks show priority actions; examples and verification steps follow where available.

Grouped issues in this report · 8

3 Medium · 5 Low

Medium (Confirmed) · **Content Security Policy (CSP) Missing**

HTTP Headers · 2 hosts

Medium (Confirmed) · **Clickjacking Protection Missing (X-Frame-Options / Frame-Ancestors)**

HTTP Headers · app.sample-company.example

Medium (Confirmed) · **Cookie Scope: Sample Company Client Id**

Cookie Analysis · sample-company.example

Low (Confirmed) · **CAA Record Missing**

DNS · sample-company.example

Low · **MIME Sniffing Protection Missing**

HTTP Headers · 2 hosts

Low · **Referrer-Policy Not Set**

HTTP Headers · 2 hosts

Low · **Permissions-Policy Not Set**

HTTP Headers · 2 hosts

Low · **MTA-STS (Email TLS)**

Email · sample-company.example

Finding 1 of 8

Content Security Policy (CSP) Missing

Medium · HTTP Headers · Failed · Confirmed · Confirmed configuration weakness

`Check: Content Security Policy (CSP) missing`

Affected hosts (2)

elements.sample-company.example, app.sample-company.example

What this means

Your site sends no Content-Security-Policy header. Without CSP there is no browser-enforced resource allowlist to limit the impact of injected markup or scripts. CSP does not invent XSS by itself; it reduces how far an injection can reach.

Risk

Medium. Raises impact of XSS and supply-chain attacks if another flaw exists.

Urgency

Plan within 30 days; not an emergency on its own.

Technical evidence

elements.sample-company.example	Failed
app.sample-company.example	Failed

Priority action

1. Inventory third-party scripts (analytics, chat widgets, payment SDKs).
2. Deploy CSP in report-only mode first and review browser console violations.
3. Tighten directives, then switch to enforcing mode.

Example

```
Content-Security-Policy-Report-Only: default-src 'self'; script-src 'self'
https://www.googletagmanager.com; style-src 'self' 'unsafe-inline'; img-src 'self' data: https:;
frame-ancestors 'none'; base-uri 'self'; form-action 'self'
```

Verify the fix

Repeat for every affected host (2): elements.sample-company.example, app.sample-company.example

```
curl.exe -sI https://elements.sample-company.example | findstr /I content-security-policy
Linux/macOS: curl -sI https://elements.sample-company.example | grep -i content-security-policy
Or use browser DevTools → Network → document response headers. Review report-only violations,
fix legitimate app breakages, then enforce once expected user flows are clean.
This example checks one host. Repeat the same command for every affected host listed above.
```

What could break

Strict script-src can break inline scripts, tag managers, and payment widgets. Start with Content-Security-Policy-Report-Only. Extensions, bots, and third-party noise may produce violations that are not your app; focus on flows you control.

Finding 2 of 8

Clickjacking Protection Missing (X-Frame-Options / Frame-Ancestors)

Medium · HTTP Headers · Failed · Confirmed · Confirmed configuration weakness · Host: app.sample-company.example

`Check: Clickjacking protection missing (X-Frame-Options / frame-ancestors)`

What this means

Your pages can be embedded in an iframe on another site. Attackers use this to overlay invisible frames and trick users into clicking actions they did not intend.

Risk

Medium. Useful for account takeover when combined with social engineering.

Urgency

Fix within 30 days, sooner on admin or payment flows.

Technical evidence

Header	`x-frame-options`
Present	`No`
Checked Url	`https://app.sample-company.example/`

Priority action

Add X-Frame-Options: DENY (or SAMEORIGIN if you embed your own pages). Prefer CSP frame-ancestors 'none' or 'self' for modern browsers.

Example

```
X-Frame-Options: DENY
Content-Security-Policy: frame-ancestors 'none'
```

Verify the fix

```
curl -sI https://app.sample-company.example | grep -iE 'x-frame-options|frame-ancestors'
Windows: curl.exe -I https://app.sample-company.example
```

What could break

DENY breaks legitimate embeds (payment iframes, partner widgets, help desks). Use SAMEORIGIN or an explicit frame-ancestors allowlist instead.

Finding 3 of 8

Cookie Scope: Sample Company Client Id

Medium · Cookie Analysis · Warning · Confirmed · Confirmed configuration weakness · Host: sample-company.example

`Check: Cookie Scope: sample_company_client_id`

What this means

A cookie is set with a Domain attribute that covers the whole registrable domain, so every subdomain can receive it. A compromised subdomain could steal application or login-session cookies.

Risk	Urgency
Medium on sites with login or session cookies.	Fix within 2 weeks for session and auth cookies.

Technical evidence

Cookie	`sample_company_client_id`
Domain	`.sample-company.example`
Scope Issue	`overly_broad_subdomain`

Priority action

Scope the cookie to the most specific host possible (omit Domain, or set it only to the exact application host). For the strongest host-only binding, rename to a __Host- prefix cookie and meet all __Host- requirements together: Secure must be set, Path must be /, Domain must be omitted, and the cookie must be set over HTTPS. Renaming alone is not enough - browsers reject __Host- cookies that omit any of these rules.

Example

```
Set-Cookie: __Host-session=...; Secure; HttpOnly; Path=/; SameSite=Lax
(no Domain attribute; served only over HTTPS)
```

Verify the fix

```
Browser DevTools → Application → Cookies. Confirm Domain is host-only (or empty), Path=/, Secure is set, and the name uses __Host- only when all rules are met.
Windows: curl.exe -sI https://sample-company.example
Linux/macOS: curl -sI https://sample-company.example
```

What could break

Do not treat a __Host- rename as a cosmetic change - missing Secure, Path=/, or including Domain will prevent the cookie from being stored. Over-broad Domain on login/session cookies increases account-takeover impact if any subdomain is compromised; this is a…

Finding 4 of 8

CAA Record Missing

Low · DNS · Warning · Confirmed · Confirmed configuration weakness · Host: sample-company.example

`Check: CAA record missing`

What this means

No CAA DNS records were found for sample-company.example. CAA does not replace domain validation; it tells cooperating certificate authorities which issuers you authorise after normal validation. Without CAA, you forgo that issuance allowlist signal.

Risk	Urgency
Low. Niche attack, but cheap insurance against mis-issuance.	Add when renewing certificates or within 90 days.

Technical evidence

Query	`sample-company.example`
Record Type	`CAA`
Records Found	`None`

Priority action

CAA inherits from the apex to subdomains unless a hostname publishes its own CAA records. Different hosts in this scan used different CAs (pki.goog, amazon.com, letsencrypt.org). Publish apex CAA only if every subdomain should inherit that full allowlist; otherwise set hostname-specific CAA using the issuer observed on each host (see example).

Example

```
CAA records inherit from parent names unless a hostname publishes its own CAA set. An apex CAA policy
therefore applies to every subdomain that does not override it.

Different hosts in this scan used different certificate authorities. Only publish a single apex CAA
allowlist if every subdomain should inherit those issuers.
Shared apex policy covering all observed issuers (pki.goog, amazon.com, letsencrypt.org) - use only
when inheritance is intentional:
0 issue "pki.goog"
0 issue "amazon.com"
0 issue "letsencrypt.org"
Optional wildcard block:
0 issuewild ";"

Otherwise publish hostname-specific CAA for the issuer actually observed on each host:
- api.sample-company.example: 0 issue "pki.goog"
- s3.sample-company.example: 0 issue "amazon.com"
- status.sample-company.example: 0 issue "letsencrypt.org"
- app.sample-company.example: 0 issue "pki.goog"
- blog.sample-company.example: 0 issue "pki.goog"
- careers.sample-company.example: 0 issue "pki.goog"
- community.sample-company.example: 0 issue "pki.goog"
- intranet.sample-company.example: 0 issue "pki.goog"
- sample-company.example: 0 issue "pki.goog"
- support.sample-company.example: 0 issue "pki.goog"
- www.sample-company.example…
```

Verify the fix

```
Windows: Resolve-DnsName sample-company.example -Type CAA
Linux/macOS: dig CAA sample-company.example +short
```

What could break

Omitting a CA you use will block renewals from that CA until DNS is updated.

Do not use issuewild ";" if you need wildcard certificates; that entry blocks wildcard issuance.

Finding 5 of 8

MIME Sniffing Protection Missing

Low · HTTP Headers · Failed · Confirmed · Confirmed configuration weakness

`Check: MIME sniffing protection missing`

Affected hosts (2)

elements.sample-company.example, app.sample-company.example

What this means

Without X-Content-Type-Options: nosniff, browsers may guess content types and treat uploaded or mislabeled files as executable content.

Risk

Low to medium. Mostly relevant if users can upload files or you serve user content.

Urgency

Fix in the next maintenance window.

Technical evidence

elements.sample-company.example	`Failed`
app.sample-company.example	`Failed`

Priority action

Add X-Content-Type-Options: nosniff on all HTML and API responses.

Example

```
X-Content-Type-Options: nosniff
```

Verify the fix

Repeat for every affected host (2): elements.sample-company.example, app.sample-company.example

```
curl -sI https://elements.sample-company.example | grep -i x-content-type-options
Windows: curl.exe -I https://elements.sample-company.example
This example checks one host. Repeat the same command for every affected host listed above.
```

What could break

Rarely breaks sites. Legacy IE behavior differs; nosniff is still recommended.

Finding 6 of 8

Referrer-Policy Not Set

Low · HTTP Headers · Failed · Confirmed · Confirmed configuration weakness

`Check: Referrer-Policy not set`

Affected hosts (2)

elements.sample-company.example, app.sample-company.example

What this means

No Referrer-Policy header is set, so referrer behaviour falls back to browser defaults. Modern browsers usually default to strict-origin-when-cross-origin, but an explicit header is still recommended for consistency and older or embedded clients.

Risk

Low. Privacy and accidental secret leakage in URL parameters on non-default clients.

Urgency

Fix within 60 days.

Technical evidence

elements.sample-company.example	`Failed`
app.sample-company.example	`Failed`

Priority action

Set Referrer-Policy: strict-origin-when-cross-origin (or stricter).

Example

```
Referrer-Policy: strict-origin-when-cross-origin
```

Verify the fix

Repeat for every affected host (2): elements.sample-company.example, app.sample-company.example

```
curl -sI https://elements.sample-company.example | grep -i referrer-policy
Windows: curl.exe -I https://elements.sample-company.example
This example checks one host. Repeat the same command for every affected host listed above.
```

What could break

strict-origin-when-cross-origin can reduce analytics referrer data.

Adjust if marketing relies on full referrer URLs.

Finding 7 of 8

Permissions-Policy Not Set

Low · HTTP Headers · Failed · Confirmed · Confirmed configuration weakness

`Check: Permissions-Policy not set`

Affected hosts (2)

elements.sample-company.example, app.sample-company.example

What this means

Browser features (camera, microphone, geolocation, payment APIs) are not restricted at the HTTP layer. Compromised third-party scripts could request sensitive permissions.

Risk

Low. Defense-in-depth for sites with many third-party scripts.

Urgency

Fix within 60 days.

Technical evidence

elements.sample-company.example	`Failed`
app.sample-company.example	`Failed`

Priority action

Deny features you do not use; allow only what embedded widgets need.

Example

```
Permissions-Policy: camera=(), microphone=(), geolocation=(), payment=(self "https://js.stripe.com")
```

Verify the fix

Repeat for every affected host (2): elements.sample-company.example, app.sample-company.example

```
curl -sI https://elements.sample-company.example | grep -i permissions-policy
Windows: curl.exe -I https://elements.sample-company.example
This example checks one host. Repeat the same command for every affected host listed above.
```

What could break

Overly strict policies can break video chat, maps, or payment SDKs.

Finding 8 of 8

MTA-STS (Email TLS)

Low · Email · Warning · Confirmed · Confirmed configuration weakness · Host: sample-company.example

`Check: MTA-STS (Email TLS)`

What this means

Inbound email may still use TLS, but without MTA-STS it is not strictly enforced and is more vulnerable to downgrade attacks.

Risk

Low to medium. Opportunistic TLS often works, but attackers can strip it.

Urgency

Plan within 30-90 days for mail domains you control.

Technical evidence

Query	`_mta-sts.sample-company.example`
Record Type	`TXT`
Records Found	`None`

Priority action

1) Publish a DNS TXT record at _mta-sts.sample-company.example (for example v=STSv1; id=YYYYMMDD). 2) Host the policy file at https://mta-sts.sample-company.example/.well-known/mta-sts.txt over HTTPS with a valid certificate for mta-sts.sample-company.example. 3) Include the required policy fields: version: STSv1, mode: testing|enforce, one or more mx: lines matching your MX hosts, and max_age: (seconds). 4) Start with mode: testing so failures are reported without rejecting mail, confirm delivery looks healthy, t…

Example

```
_mta-sts.sample-company.example. TXT "v=STSv1; id=20260101"
https://mta-sts.sample-company.example/.well-known/mta-sts.txt contents:
version: STSv1
mode: testing
mx: aspmx.l.google.com
max_age: 86400
```

Verify the fix

```
Windows: Resolve-DnsName _mta-sts.sample-company.example -Type TXT
Linux/macOS: dig TXT _mta-sts.sample-company.example +short
Windows: curl.exe -sI https://mta-sts.sample-company.example/.well-known/mta-sts.txt
Linux/macOS: curl -sI https://mta-sts.sample-company.example/.well-known/mta-sts.txt
Fetch the body and confirm version, mode, mx, and max_age are present.
```

What could break

Start in mode: testing before mode: enforce so misconfigured MX lines
do not block inbound mail.
The policy hostname mta-sts.sample-company.example needs its own valid
HTTPS certificate.
mx: values must match your real MX hosts.

08 · Successful check instances

Showing 40 of 51. Omitted: Typosquat lookalikes, Login panels, HTTP to HTTPS Redirect, robots.txt, CORS Configuration, Service banners, WordPress, Open redirects, API discovery, Rate limiting, CVE lookup.

Check	Host	Evidence	Module
SPF Record	`sample-company.example`	v=spf1 include:_spf.google.com ~all	Dns
DKIM Record	`google._domainkey.sample-company.example`	DKIM record found for a known provider selector	Dns
Nameserver Redundancy	`sample-company.example`	2 nameservers configured	Dns
Mail Exchange (MX)	`sample-company.example`	7 MX record(s) configured	Dns
DNSSEC	`sample-company.example`	DNSSEC is enabled for this domain	Dns
Certificate Expiry	`sample-company.example`	Certificate valid for 41 more days	Ssl
Certificate Authority	`sample-company.example`	Certificate chain trusted	Ssl
Domain Match	`sample-company.example`	Certificate properly covers sample-company.example	Ssl
Key Strength	`sample-company.example`	Key: 256-bit ECDSA	Ssl
TLS 1.3 Support	`sample-company.example`	Server negotiates TLS 1.3 on the primary HTTPS port	Ssl
Cipher Strength	`sample-company.example`	Cipher: TLS_AES_256_GCM_SHA384 (256 bits)	Ssl
Certificate Expiry	`api.sample-company.example`	Certificate valid for 41 more days	Ssl
Certificate Authority	`api.sample-company.example`	Certificate chain trusted	Ssl
Domain Match	`www.sample-company.example`	Certificate properly covers www.sample-company.example	Ssl
Domain Match	`api.sample-company.example`	Certificate properly covers api.sample-company.example	Ssl

Domain Match	app.sample-company.example	Certificate properly covers app.sample-company.example	Ssl
Domain Match	blog.sample-company.example	Certificate properly covers blog.sample-company.example	Ssl
Domain Match	careers. sample-company. example	Certificate properly covers careers.sample-company.example	Ssl
Domain Match	community. sample-company. example	Certificate properly covers community.sample-company.example	Ssl
Domain Match	intranet. sample-company. example	Certificate properly covers intranet.sample-company.example	Ssl
Domain Match	s3.sample-company.example	Certificate properly covers s3.sample-company.example	Ssl
Domain Match	status. sample-company. example	Certificate properly covers status.sample-company.example	Ssl
Domain Match	support. sample-company. example	Certificate properly covers support.sample-company.example	Ssl
HTTP Strict Transport Security (HSTS)	sample-company.example	HTTP Strict Transport Security (HSTS) is configured	Header
X-Frame-Options	sample-company.example	X-Frame-Options is configured	Header
X-XSS-Protection	sample-company.example	X-XSS-Protection is configured	Header
HTTP Strict Transport Security (HSTS)	app.sample-company.example	HTTP Strict Transport Security (HSTS) is configured	Header
HTTP Strict Transport Security (HSTS)	www.sample-company.example	HTTP Strict Transport Security (HSTS) is configured	Header
X-Frame-Options	www.sample-company.example	X-Frame-Options is configured	Header
X-XSS-Protection	www.sample-company.example	X-XSS-Protection is configured	Header
HTTP Strict Transport Security (HSTS)	careers. sample-company. example	HTTP Strict Transport Security (HSTS) is configured	Header
Exposed: /.well-known/security.txt	sample-company.example	security.txt found	Exposed Files

Directory Listing	sample-company.example	No directory listings detected on common paths	Dir Listing
Cloud Storage Exposure	sample-company.example	No publicly listable cloud storage buckets found for common naming patterns	Cloud Storage
DMARC Policy Strength	sample-company.example	DMARC policy is 'quarantine' at 100%	Email Deep
BIMI (Brand Authentication)	sample-company.example	BIMI record found with logo and VMC (Verified Mark Certificate)	Email Deep
SMTP TLS Reporting (TLSRPT)	sample-company.example	TLSRPT record configured	Email Deep
SPF Lookup Limit	sample-company.example	SPF record uses 1/10 allowed DNS lookups	Email Deep
Email harvesting	sample-company.example	No public email addresses harvested from the site during this scan	Email Harvest
JS secrets	sample-company.example	No API keys or credential patterns matched in scanned JavaScript	Js Secrets

09 · Essential Eight indicators

External risk indicators only. This is not an Essential Eight maturity assessment. ACSC assessments require scoped checks of control implementation and effectiveness inside your environment. EightScope can only report what is visible from the public internet.

Patch Applications · No external evidence detected

What this control covers

Known CVEs and disclosed application/library versions on public assets. Outdated TLS protocols or unexpected ports alone are not mapped here without version or CVE evidence.

Findings / evidence

· No public CVE matches or disclosed vulnerable application versions detected externally

Limitation

We only see internet-facing assets. Internal app patching and endpoint updates happen inside your network and are not visible externally.

Patch Operating Systems · No external evidence detected

What this control covers

Server OS version hints from banners and HTTP headers.

Findings / evidence

· No server OS version disclosure detected in banners or headers

Limitation

Most OS patching is invisible from outside. We only detect version strings when servers disclose them.

Multi Factor Authentication · Not externally assessable

Why this cannot be assessed externally

MFA on VPN, Microsoft 365, SaaS, and staff login flows.

Findings / evidence

No external signals recorded.

Limitation

MFA is enforced inside identity providers and applications. We cannot authenticate as your users or read IdP policy from the outside.

Restrict Admin Privileges · No external evidence detected

What this control covers

Exposed admin panels, default admin paths, and sensitive files on the web.

Findings / evidence

· No exposed admin panels or critical sensitive files detected

Limitation

We can spot exposed admin interfaces, but not who has admin rights internally or how privileges are assigned in Active Directory or cloud IAM.

Application Control · Not externally assessable

Why this cannot be assessed externally

Application whitelisting on endpoints and servers.

Findings / evidence

No external signals recorded.

Limitation

Whitelisting runs on devices and servers. External scanning has no visibility into installed software policies or execution controls.

Restrict Office Macros · Not externally assessable

Why this cannot be assessed externally

Macro policies in Microsoft 365 / Office.

Findings / evidence

No external signals recorded.

Limitation

Macro settings are configured in Microsoft 365 admin centres and Group Policy. Not on your public website.

User Application Hardening · External weaknesses observed

What this control covers

HTTP security headers (CSP, frame controls, and related), cookie flags, and CORS on web apps.

Findings / evidence

· No Content Security Policy. The site is more vulnerable to XSS attacks.
· X-Content-Type-Options not set. Browsers may MIME-sniff responses.
· No Referrer-Policy header. Behaviour falls back to browser defaults; an explicit header is recommended for consistency.
· No Permissions-Policy header. Browser features are unrestricted.
· X-Frame-Options not set. The site may be vulnerable to clickjacking.

Limitation

Headers reflect web-app hardening only. Browser policies, extensions, and endpoint hardening on staff devices are internal controls.

Regular Backups · Not externally assessable

Why this cannot be assessed externally

Backup schedules, retention, and restore testing.

Findings / evidence

No external signals recorded.

Limitation

Backups run inside your infrastructure. We cannot verify backup jobs, off-site copies, or restore drills from DNS/HTTPS checks alone.

External risk indicators only. This is not an Essential Eight maturity assessment. ACSC assessments require scoped checks of control implementation and effectiveness inside your environment. EightScope can only report what is visible from the public internet.

Scan coverage

Modules run during this scan and known limitations.

27 modules in scope: 26 completed, 1 not assessed

Asset-level TLS/header checks on discovered hosts are expansions of the TLS and HTTP header modules, not extra marketed full-scan modules.

Asset inventory

Discovered: **13** · Reachable: **13** · Fully assessed: **11** · Partially assessed: **1** · Error: **1** · Unassessed: **0**
TLS attempted: **12** · completed: **11** · errors: **1** · unassessed: **1**

CDN classification is shared across hosts on the same edge IPs (ranges, headers, and CDN PTR/CNAME evidence). Observed edge providers in this scan: CloudFront, Cloudflare. Different providers (e.g. Cloudflare vs CloudFront) remain distinct by evidence.
Asset totals are recalculated from TLS and header module outcomes. Fully assessed = both modules completed. Partially assessed = one module completed. Error = a module started but failed. Unassessed = not selected or not run. TLS completed counts only successful certificate captures - errors are listed separately and are not treated as completed.

- Port scan: top 1000 common TCP ports (top_1000). Deep port scan (all 65535 TCP ports) is a separate full-scan add-on.
- UDP: limited probe on ports 53, 123, 161 when port scan runs.
- Subdomain discovery combines passive sources (Certificate Transparency and, when configured, VirusTotal / SecurityTrails) with active DNS wordlist resolution, wildcard DNS testing, and HTTP/HTTPS reachability probing.
- EightScope does not perform destructive exploitation, authenticated application testing or full DAST. WAF detection may send harmless encoded trigger strings to observe blocking behaviour.
- External surface checks only: no authenticated login testing, form fuzzing, payment flows, or in-app API exploitation. DNS wordlist enumeration and WAF trigger probes are active validation, not zero-probe scanning.
- Typosquat: checked 80 lookalike permutations. Not exhaustive monitoring.
- TLS: certificate and protocol audit. Enable deep SSL for cipher enumeration and OCSP checks.
- Discovery mode: Passive sources plus active validation (Certificate Transparency + DNS wordlist / reachability). VirusTotal / SecurityTrails provider datasets are not configured.
- Asset-level TLS and HTTP header checks assess the verified apex plus up to 20 selected non-apex hostnames (priority: sensitive names, then reachable HTTPS/HTTP). Discovered hosts beyond that cap are listed but not fully scanned; they are not treated as secure.
- Quick scans assess apex TLS/headers only. Standard and full scans do not claim every discovered subdomain was fully assessed.
- Malware / Safe Browsing: not assessed (provider not configured).