Domainscan OSINT Report

Domain Surface Intelligence

Passive subdomains	HTTP 200 responses	External hosts
10	8	4

Executive Summary

This assessment maps DNS and TLS for example-corp.io, summarizes discovered subdomains and live HTTP responses, classifies environments and technology fingerprints, and lists external hostnames observed during page load. Machine-readable detail is available in report.json.

About Infrastructure

Authoritative and apex DNS data from the scan.

Record	Value
A	203.0.113.10, 203.0.113.11
AAAA	2001:db8:abcd::1
NS	ns1.example.net., ns2.example.net.
CNAME	-
SOA	ns1.example.net. hostmaster.example.net. 2026041601 3600 600 86400 300
TXT	v=spf1 include:_spf.example.net ~all
TXT	google-site-verification=demo-token

MX host	Preference
mail.example-corp.io.	10
smtp-backup.example.net.	20

Email signal	Detail
SPF	v=spf1 include:_spf.example.net ~all

Associated hosts (passive): 10

About Certification (TLS)

Field	Value
Subject CN	www.example-corp.io
Issuer	R3
Valid not before (UTC)	2026-03-01T00:00:00Z
Valid not after (UTC)	2026-05-30T23:59:59Z
TLS version	TLS 1.3
Cipher suite	TLS_AES_128_GCM_SHA256
ALPN / negotiated	h2
Signature algorithm	ECDSA-SHA256
Verified chains (best-effort)	1
SAN DNS names	example-corp.io, www.example-corp.io

Leaf certificate material from a single tcp/443 handshake to the primary hostname.

robots.txt

Disallow paths apply to the wildcard user-agent group (User-agent: *) on the apex host.

Source: https://example-corp.io/robots.txt

Disallow path
/admin/
/api/internal/
/tmp/

Sitemap URL
https://example-corp.io/sitemap.xml

Cloud enumeration

Keywords: examplecorp, example-corp (48 name candidates)

Cloud	Resource	Access	Target
AWS	S3 bucket	public	examplecorp-assets.s3.amazonaws.com
Azure	Blob storage	unknown	examplecorp.blob.core.windows.net

About Assets

Environment is inferred from hostnames. Type is Website vs API from Content-Type, URL patterns, and technology hints.

Top technologies

nginx · Cloudflare · PHP · Apache HTTP Server · Bootstrap · Google Analytics · Google Tag Manager · HSTS · HTTP/3 · jQuery

Asset inventory

Asset	Environment	Website (URL)	Status	Type
api.example-corp.io	Production	https://api.example-corp.io/v1/health	200	API
blog.example-corp.io	Production	https://blog.example-corp.io/	200	Website
cdn.example-corp.io	Production	https://cdn.example-corp.io/	200	Website
dev.example-corp.io	Development	https://dev.example-corp.io/	302	Website
mail.example-corp.io	Production	https://mail.example-corp.io/	200	Website
shop.example-corp.io	Production	https://shop.example-corp.io/	200	Website
staging.example-corp.io	Staging	https://staging.example-corp.io/	200	Website
status.example-corp.io	Production	https://status.example-corp.io/	200	Website
vpn.example-corp.io	Production	https://vpn.example-corp.io/	403	Website
www.example-corp.io	Production	https://www.example-corp.io/	200	Website

Vendors (external hostnames)

Full hostname as observed in network traffic. Type: API vs Non-API (from Content-Type and URL heuristics).

External hostname	Type
api.segment.io	API
cdn.jsdelivr.net	Non-API
fonts.googleapis.com	Non-API
www.googletagmanager.com	Non-API

CMS - WordPress

WordPress asset	Plugins / themes	Users
https://blog.example-cor...	contact-form-7, yoast-seo | themes: twen...	editor