URLScanner.online

Security Scan Report

thehalara.com

18 March 2026 at 19:06 · 53.3s

64
/100

https://thehalara.com/

SUSPICIOUS **AI: 25/100 · MEDIUM RISK**

Resolved IP: 65.8.202.123 · Server: —

MALWARE	SAFE BROWSING	SSL	DOMAIN AGE
Clean	Clean	Valid	1972d

● THREAT DETECTION

URLhaus	CLEAN
Google Safe Browsing	CLEAN
Spamhaus	NOT LISTED
SURBL	NOT LISTED
Checked IP	`65.8.202.70`

● SSL CERTIFICATE

Status	VALID
Protocol	`TLSv1.3`
Cipher Suite	`TLS_AES_128_GCM_SHA256`
Subject	thehalara.com
Issuer	Amazon RSA 2048 M03 (Amazon)
Valid From	Aug 9 00:00:00 2025 GMT
Expires	Sep 7 23:59:59 2026 GMT (173 days remaining)
HSTS	Enabled `max-age=63072000; includeSubDomains; preload`
OCSP	unknown
Key	RSA 2048 bits
Serial Number	`0698CFE6B6C2290230D622BAA5CB567C`
SANs	thehalara.com

● HTTP SECURITY HEADERS

Status: **200 OK** · Final URL: `https://eur.halara.com/?switchSite=M_To_EUR&_switch_domain=ES_EUR_es` · 2 redirects

HEADER	STATUS	VALUE
HSTS	present	`max-age=63072000; includeSubDomains; preload`
X-Content-Type-Options	missing	–
X-Frame-Options	present	`ALLOW-FROM https://crm.test.doublefs.com`
CSP	present	`frame-ancestors 'self' https://crm.test.doublefs.com https://crm.prod.doublefs.com;`
Referrer-Policy	missing	–
Permissions-Policy	missing	–
COOP	missing	–
COEP	missing	–
CORP	missing	–
X-XSS-Protection	missing	–

DNS RECORDS

19 records

Type	Name	Value	TTL
A	thehalara.com	65.8.202.123	59
A	thehalara.com	65.8.202.22	59
A	thehalara.com	65.8.202.70	59
A	thehalara.com	65.8.202.2	59
MX	thehalara.com	inbound-smtp.us-west-2.amazonaws.com	0
NS	thehalara.com	ns-1633.awsdns-12.co.uk	0
NS	thehalara.com	ns-330.awsdns-41.com	0
NS	thehalara.com	ns-677.awsdns-20.net	0
NS	thehalara.com	ns-1181.awsdns-19.org	0
TXT	thehalara.com	globalsign-domain-verification=FD6BE1E6BDF910FA2A0C53913B443418	0
TXT	thehalara.com	google-site-verification=72OmybPk9vj4jA2DEGipBcIaPQf2975BH4diI1dzLo0	0
TXT	thehalara.com	google-site-verification=RijZph0vgfakbP060clbA3soTbjppac9JaJopE1CKWQ	0
TXT	thehalara.com	globalsign-domain-verification=lnA6c_87C_nWD8MyPIucBXZSh-7ttTX_YtfnSJ4_Kq	0
TXT	thehalara.com	google-site-verification=1lNZWHZVshR9Cl7b-_tf0OK5_YXQCWWKjGguCjjnW1k	0
TXT	thehalara.com	google-site-verification=jQDuJTV5h6zGEBX5tXZhxEIsGV-VDRycfpMI6rnkELA	0
TXT	thehalara.com	facebook-domain-verification=kafsfhbjmx9vjkp73gsnpkpe35jkio	0
TXT	thehalara.com	v=spf1 include:amazonses.com include:sendgrid.net include:shops.shopify.com include:mail.zendesk.com ~all	0
TXT	thehalara.com	klaviyo-site-verification=YjpTND	0
SOA	thehalara.com	ns-1633.awsdns-12.co.uk awsdns-hostmaster.amazon.com 1	86400

WHOIS REGISTRATION

Registrar	Dominet (HK) Limited
Registrant Org	—
Registrant Country	SG
Domain Age	1972 days
Created	2020-10-23T00:41:06Z
Updated	2025-10-18T02:00:45Z
Expires	2032-10-23T00:41:06Z
Nameservers	ns-1181.awsdns-19.org ns-1633.awsdns-12.co.uk ns-330.awsdns-41.com ns-677.awsdns-20.net

● TECHNOLOGY STACK

TECHNOLOGY	CATEGORY	CONFIDENCE	EVIDENCE
Next.js	Framework	high	Header: x-powered-by: Next.js
Shopify	E-commerce	medium	HTML pattern: cdn\.shopify\.com
Google Analytics	Analytics	medium	HTML pattern: google-analytics\.com
Google Tag Manager	Tag Manager	medium	HTML pattern: googletagmanager\.com\/gtm\.js
Facebook Pixel	Analytics	medium	HTML pattern: connect\.facebook\.net

● AI SECURITY ANALYSIS

gpt-4.1-nano · two-pass analysis

INTELLIGENCE KNOWLEDGE CHECK

UNKNOWN | Unknown — suspicious pattern | Unknown domain

The domain 'thehalara.com' does not correspond to any major brand, government, or well-known infrastructure based on training data. Its registration in Singapore with a relatively recent age (~1972 days) and lack of prominent reputation suggests it is not a trusted entity. No specific associations with malicious activity are documented, but the domain's pattern and lack of recognition warrant caution.

⚠ Lack of recognition as a major or trusted entity

⚠ No known association with reputable brands or infrastructure

⚠ Potentially new or obscure domain with limited reputation data

SCAN EVIDENCE VERDICT

25 /100 MEDIUM RISK

The domain 'thehalara.com' is unfamiliar and lacks a well-known reputation, aligning with prior intelligence indicating it is an obscure, relatively new domain. The real-time scan confirms this suspicion, showing a young domain with minimal security headers, despite a valid SSL certificate issued by Amazon. The redirect chain leads to 'eur.halara.com', an unknown destination, which raises concerns about potential deceptive or malicious intent. No blocklist flags are present, but the overall pattern suggests cautious monitoring rather than outright maliciousness.

1. Monitor the redirect chain to 'eur.halara.com' for suspicious activity or content.
2. Implement additional security headers such as X-Content-Type-Options and Referrer-Policy to improve security posture.
3. Conduct further investigation into the destination domain 'eur.halara.com' before any user interaction.
4. Consider blocking or flagging the domain for users in sensitive environments until more is known.