HACKATHON.AE 2026 · DIGITAL TRUST & CYBER-SECURE NATION

SAQR صقر

Fake government payment pages — caught while they are being set up, blocked everywhere with one click.

Team Falcon Rush · NYU Abu Dhabi

Challenge 6 · impersonation of government financial services

THE PROBLEM

Today the fake is found after the money is gone

Name registered
any registrar, any TLD

→

Certificate
free, minutes

→

SMS wave
“claim your refund within 24 h”

→

Victims pay
card · CVV · OTP relayed live

→

found here

Complaints
hours to days later

→

Takedown
one partner at a time · days

> 75%

of cyber breaches start with phishing or fraudulent messages

UAE Cyber Security Council

+35%

scam messages in one year

UAE Cyber Security Council

days

online while registrar, host and telecoms are contacted one by one

THE INSIGHT

Scammers publish their own early warning

Every HTTPS site needs a certificate. Every certificate is written to public logs within minutes. We read the same stream.



~150 / s

certificates streamed from two Google logs in our tests

1 in 3,000

names survive the cheap look-alike filter

0 citizens

no traffic taps, no phones, no browsing data

HOW IT WORKS

Sense · Assess · Qualify · Respond

01

Sense

Watch the certificate logs and forwarded messages. Keep look-alikes of official names.

CT logs · homographs · SMS / WhatsApp

02

Assess

Open the page in an isolated browser. Compare with the real one. Read what the form asks for.

visual match · emblem · card · CVV · OTP

03

Qualify

Seal the evidence: hashes, Merkle root, trusted timestamp, chain of custody.

SHA-256 · RFC 3161 · re-verifiable

04

Respond

One click by a named analyst. Seven partners at once. Audit chain for every step.

telecoms · browsers · registrar · host · banks

STAGE 1 · SENSE

150 certificates a second. One line each. The filter explains every point.

TIME	DOMAIN	ISSUER	SCORE
09:04:28	loop82.fr	Cloudflare	·
09:04:28	api.forgeunit.io	Amazon	·
09:04:28	www.rta.ae	DigiCert	official
09:04:27	textilesrefund.net	DigiCert	·
09:04:27	www.dubai-systems.com	Sectigo	·
09:04:26	zincdash.org	ZeroSSL	·
09:04:26	www.motors-echo.net	Google Trust Services	·
09:04:26	mail.harborpixel.de	Let's Encrypt	·
09:04:26	rune-kitchen.com	Cloudflare	·
09:04:26	abudhabiloop.com	Amazon	·
09:04:26	www.quillbeach.ae	GoDaddy	·

xn--tx-refund-gov-w1k.com

→ tax-refund-gov.com Cyrillic “a”

IDN homograph **+50** · brand “tax” **+25** · lure “refund” **+20** · gov cue **+10** · combination **+20**

score 100 · candidate

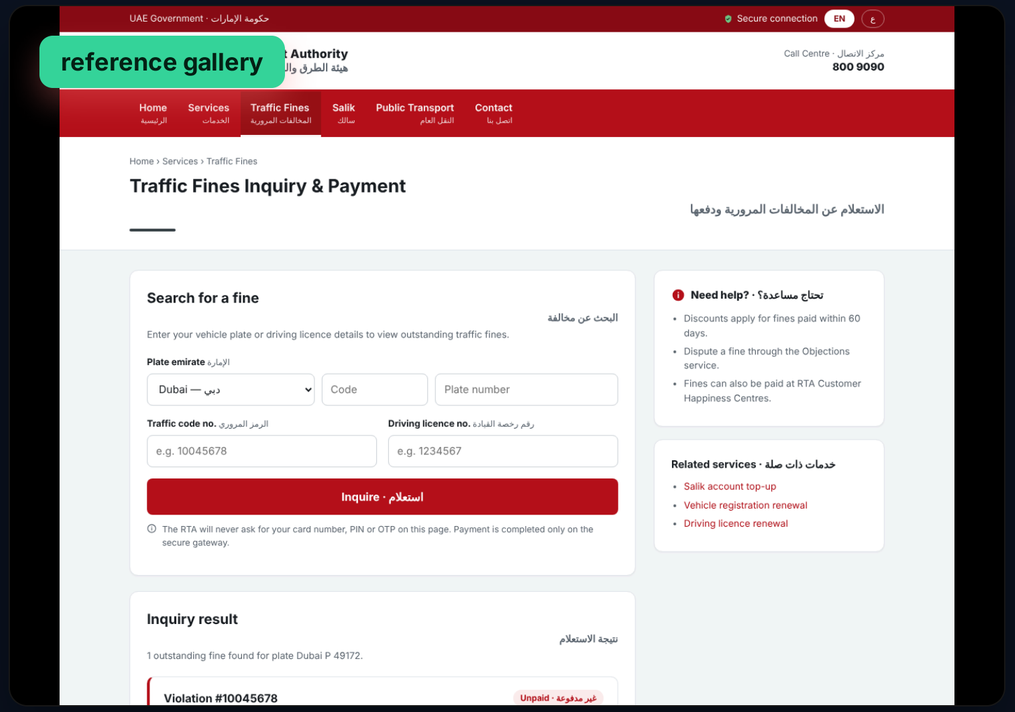
www.rta.ae

official domain — allow-listed, score 0, can never be flagged or blocked

STAGE 2 · ASSESS

Does it look official — and does it ask for a card?

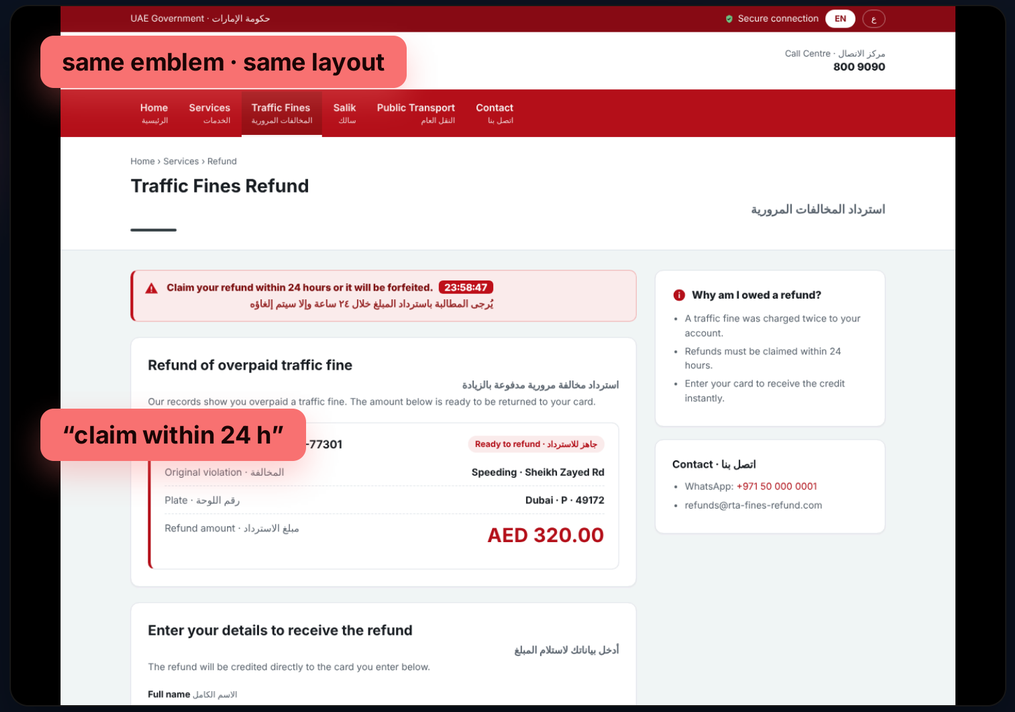
● **Reference** · `rta.ae` (demo replica)



90
RISK / 100

layout 93 %
emblem match
on demo fixtures

● **Suspect** · `rta-fines-refund.com` (demo clone)



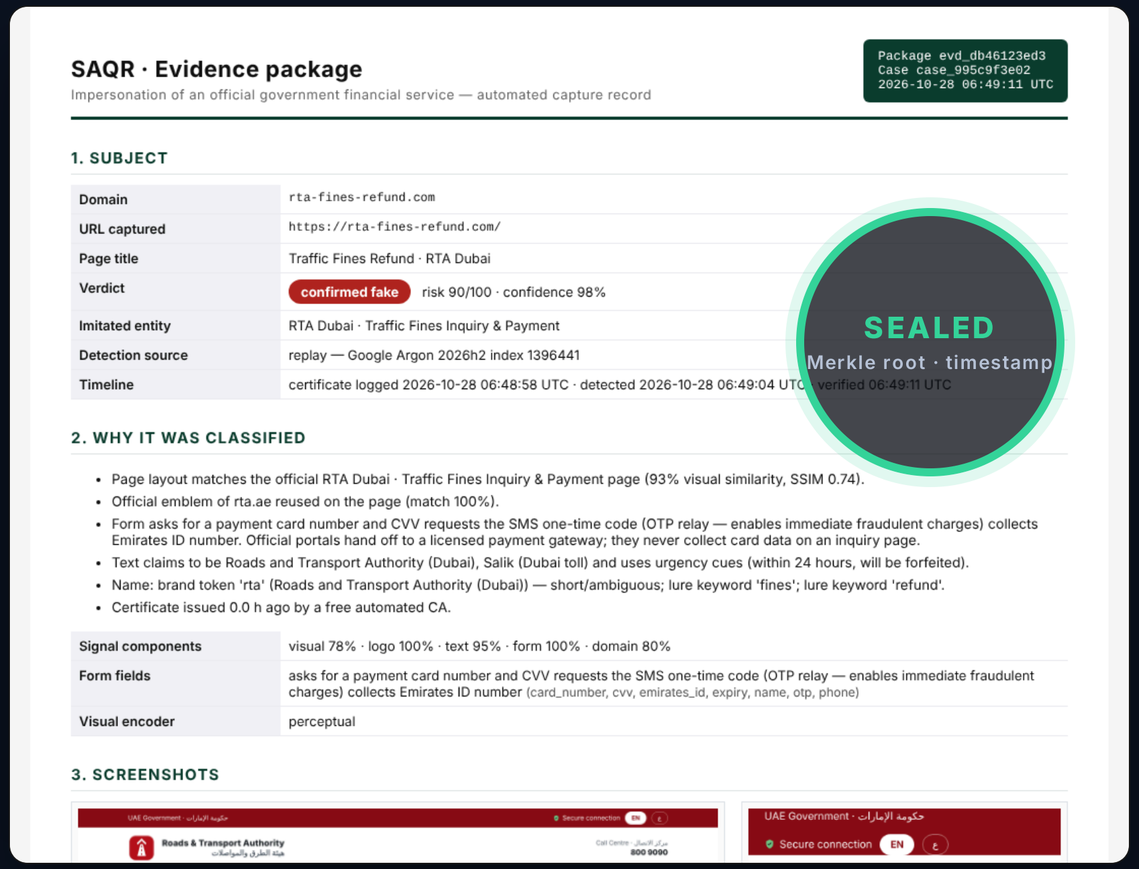
“claim within 24 h”

confirmed fake · layout copied · RTA emblem reused · collects card + OTP · certificate minutes old, free CA

gym site with the same word → cleared · evidence sealed automatically · hashes · Merkle root · timestamp

STAGE 3 · QUALIFY

Evidence sealed automatically — in about a second



SAQR · Evidence package

Impersonation of an official government financial service — automated capture record

```
Package evd_db46123ed3
Case case_995c9f3e02
2026-10-28 06:49:11 UTC
```

1. SUBJECT

Domain	rta-fines-refund.com
URL captured	https://rta-fines-refund.com/
Page title	Traffic Fines Refund · RTA Dubai
Verdict	confirmed fake · risk 90/100 · confidence 98%
Imitated entity	RTA Dubai · Traffic Fines Inquiry & Payment
Detection source	replay — Google Argon 2026h2 index 1396441
Timeline	certificate logged 2026-10-28 06:48:58 UTC · detected 2026-10-28 06:49:04 UTC · verified 06:49:11 UTC

SEALED
Merkle root · timestamp

2. WHY IT WAS CLASSIFIED

- Page layout matches the official RTA Dubai · Traffic Fines Inquiry & Payment page (93% visual similarity, SSIM 0.74).
- Official emblem of rta.ae reused on the page (match 100%).
- Form asks for a payment card number and CVV requests the SMS one-time code (OTP relay — enables immediate fraudulent charges) collects Emirates ID number. Official portals hand off to a licensed payment gateway; they never collect card data on an inquiry page.
- Text claims to be Roads and Transport Authority (Dubai), Salik (Dubai toll) and uses urgency cues (within 24 hours, will be forfeited).
- Name: brand token 'rta' (Roads and Transport Authority (Dubai)) — short/ambiguous; lure keyword 'fines'; lure keyword 'refund'.
- Certificate issued 0.0 h ago by a free automated CA.

Signal components	visual 78% · logo 100% · text 95% · form 100% · domain 80%
Form fields	asks for a payment card number and CVV requests the SMS one-time code (OTP relay — enables immediate fraudulent charges) collects Emirates ID number (card_number, cvv, emirates_id, expiry, name, otp, phone)
Visual encoder	perceptual

3. SCREENSHOTS

13
artefacts: screenshots, DOM, HAR, DNS, RDAP, certificate, hosting, IOCs

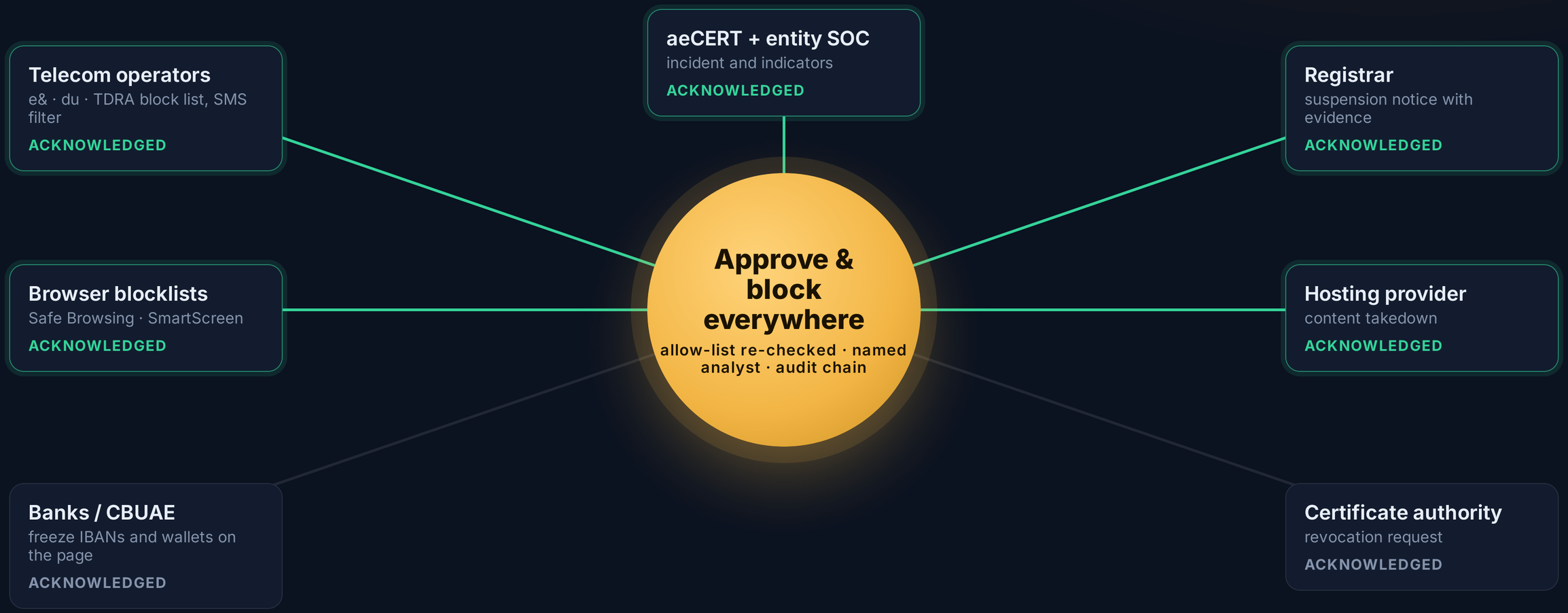
1
log entry anyone can re-fetch: log + index of the certificate that triggered it

SHA-256 every file → **Merkle root** one hash → **Timestamp** RFC 3161 → **Custody** every step

Re-verifiable offline with `saqr evidence verify` — no trust in SAQR required. Attached to every takedown request.

STAGE 4 · RESPOND

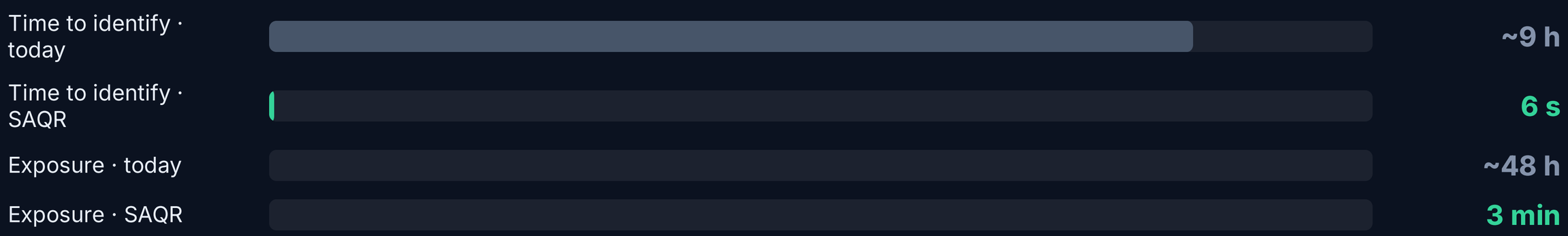
One click. Seven partners. A human decides.



TIME BUDGET · DEMO RUN

Seconds to identify. Minutes to block — including the human.





Pipeline steps measured in the offline demo; with the live feed the clock starts at the public certificate timestamp, which anyone can recompute from the log entry in the evidence package. Partner acknowledgements are simulated. Baselines are documented assumptions, to be replaced by historical case data. Targets: −70 % and −50 %.

BUILT FOR THE CONSTRAINTS

Identity, privacy, evidence, law — by design

Identity

- No citizen identity processed
- Every approval attributed to a named analyst
- UAE PASS sign-in in production

Privacy

- Only what the attacker publishes
- Reporter numbers masked and hashed
- Identifiers scrubbed from forwarded texts

Evidence

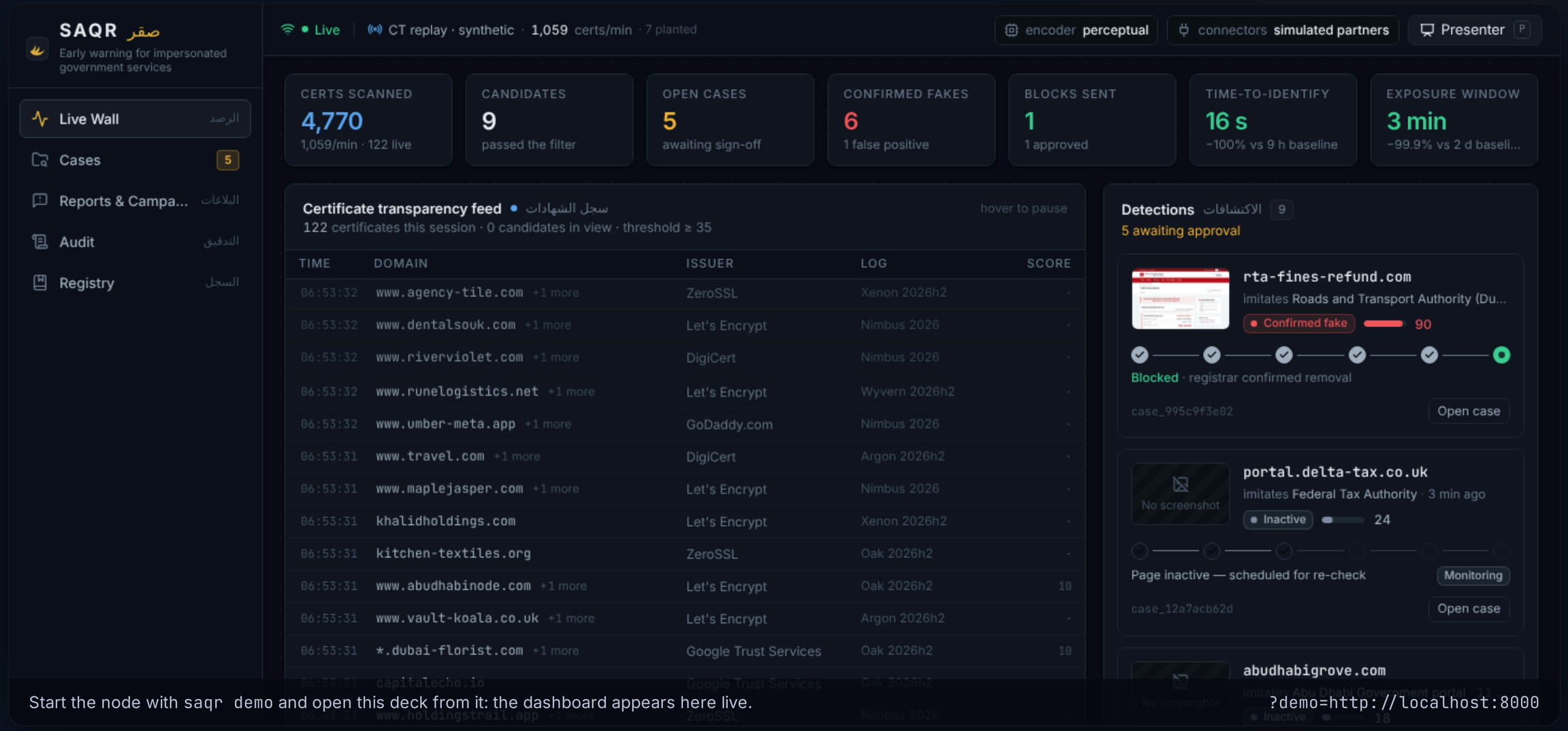
- SHA-256 · Merkle root · RFC 3161
- Append-only audit chain
- Trust Services law (46/2021)

Law

- Human sign-off before any block
- Allow-list enforced server-side
- Notices cite RAA 3.18 · BR 4.9.1.1 · Cybercrimes law (34/2021)

LIVE

Watch it happen



Start the node with `saqr demo` and open this deck from it: the dashboard appears here live.

`?demo=http://localhost:8000`

HONEST SCOPE · NEXT 90 DAYS

What it does not do yet — and what comes next

Not yet

- meaningless names, wildcard certs, free hosting → reactive path only
- partner connectors simulated (real payloads, no credentials)
- perceptual encoder in the demo · DINOv3 plugs in
- verifier evaluated on our own fixtures, not on real scam pages yet
- baselines are assumptions until historical data
- no authentication in the MVP

Next

- TDRA · e& · du · UAE Banks Federation · aeCERT · CA APIs
- DINOv3 fine-tuned on historical impersonation cases
- UAE PASS sign-in · national time-stamping authority
- citizen reporting number + WhatsApp bot
- all CT logs · registrar zone feeds · ads & social

Operate

one national node (Cyber Security Council / TDRA); each entity's SOC sees its own cases

Measure

time-to-identify and exposure per case, anchored on public log timestamps — the challenge KPIs, continuously

Extend

same pipeline for fake apps, ads and social accounts: new sensors, same verification and response

SAQR · صقر

Catch them while they set up. Block them everywhere with one click.

TRY IT · LIVE SYSTEM, DECK, CODE

saqr-hackathon.pages.dev

Team Falcon Rush · NYU Abu Dhabi
hackathon.ae 2026

شكراً