

Brand Protection | Platform module

Find and remove the fakes that use your name.

Cybersee monitors domains, social media, app stores and ads for impersonation of your brand, executives and apps. Every case is verified and taken down.

Brand threats, acme.sa

Monitoring

acme-login.help
Phishing site, live

Critical

acme-pay.shop
Lookalike domain

High

@acme_support_sa
Fake support account

High

Takedown requested for acme-login.help

In progress

WHY IT MATTERS

What you get with Brand Protection



Protect your customers

Stop fake sites, accounts and apps from stealing your customers' money and data.



Catch phishing early

Lookalike domains are flagged as they are registered, before the campaign launches.



Protect your leaders

Fake profiles of executives and VIPs are found and removed across platforms.

WHERE WE LOOK

Domain registrations

Certificate transparency

X

Instagram

TikTok

Facebook

LinkedIn

Snapchat

Google Play

App Store

Third-party app stores

Telegram

WhatsApp

Search and ad libraries

BUILT FOR SAUDI ORGANIZATIONS

Local by design



Hosted in Saudi Arabia

Customer data is stored and processed inside the Kingdom.



Arabic-native

Arabic channels, forums and slang are monitored natively.



Built for local regulation

Supports NCA ECC, SAMA CSF and PDPL programs.

COVERAGE

What Brand Protection detects



Lookalike and typosquat domains

New domains and certificates similar to your brand, including Arabic transliterations.



Phishing sites and kits

Live pages copying your login, payment or OTP screens, with kit fingerprints.



Fake social accounts

Impersonating profiles and pages on X, Instagram, TikTok, Facebook, LinkedIn and Snapchat.



Fake mobile apps

Unofficial apps using your name or logo on official and third-party stores.



Executive impersonation

Fake profiles and messages targeting your leaders, employees and partners.



Fraudulent ads and offers

Scam promotions, fake prizes and giveaways using your brand.

HOW IT WORKS

See. Verify. Remove.

Tools that only find threats hand you more work. Cybersee closes the loop.

1 See

Continuous monitoring

Domains, platforms, stores and ads are scanned continuously for your brand assets.

2 Verify

Analyst verification

Evidence is captured automatically and every case is confirmed by an analyst.

3 Remove

Takedown and watch

We request removal and keep watching for the threat to return.

INTEGRATIONS

Fits the stack you already run

Verified alerts arrive with evidence in the tools your team already uses.

Splunk

Microsoft Sentinel

IBM QRadar

ServiceNow

Jira

Slack

Microsoft Teams

Email

REST API

Webhooks

DELIVERABLES

What your team receives

**Verified alerts with evidence**

Screenshots, domain records and hosting details for every case.

**Takedown handling**

Requests to registrars, hosts and platforms, tracked until offline.

**Dashboards and reports**

Live status, trends and monthly reports for management.

**Integrations and API**

Alerts in your SIEM, ticketing and chat tools.

GET STARTED

Secure your external attack surface in 3 steps

1 Sign up**Tell us what to protect**

Share your domains, brands, apps and key executives. We size your coverage and recommend a plan.

2 Proof of concept**Test it on your real assets**

We run Cybersee on your own domains and brands, then review the verified findings with you.

3 Go live**Monitoring and takedowns**

Connect your SIEM and ticketing tools, and our analysts start monitoring and removing threats.

PLANS

Coverage sized to your organization

Starter

For teams that want to see their exposure and try the platform themselves. Free trial, then monthly.

Business

Every module with analyst-verified alerts, takedowns and integrations. Annual plan.

Enterprise

Unlimited domains and brands, executive protection, a dedicated analyst and custom reporting.

See what attackers already know about your company.

Book a 30-minute call for a walkthrough and a proof of concept on your real assets, or run a free scan at Cybersee Labs.

cybersee.ioinfo@cybersee.io