

Dark Web Intelligence | Platform module

Know when your data reaches the dark web.

Cybersee watches underground forums, markets, stealer logs and Arabic and English Telegram channels for your leaked credentials, data and network access, and alerts you before attackers use them.

Stealer log detected**Critical**

Device LAPTOP-9K2F, Windows 11
Malware RedLine stealer
Accounts vpn.acme.sa, mail.acme.sa, crm.acme.sa
Source Stealer log market, 2 hours ago

URL: https://vpn.acme.sa/login
USER: f.alqahtani@acme.sa
PASS: (session cookies: 14)

Analyst verified, password reset recommended

Verified**WHY IT MATTERS**

What you get with Dark Web Intelligence

**Stop account takeover**

Leaked employee credentials are found early so you can reset them before they are used.

**Catch access brokers**

Know when someone is selling access to your network.

**Hear the chatter**

Arabic and English mentions of your company, read in context.

WHERE WE LOOK

Breach corpora

Stealer log markets

Underground forums

Dark web marketplaces

Ransomware leak sites

Telegram channels

Paste sites

Combo lists

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 Dark Web Intelligence detects

**Leaked credentials**

Employee and customer accounts exposed in breaches, combo lists and pastes.

**Stealer logs**

Infected devices with saved logins and session cookies for your systems.

**Data for sale**

Databases and documents from your company offered on markets and forums.

**Access for sale**

VPN, RDP and admin access to your network sold by initial access brokers.

**Ransomware leak sites**

Your company or suppliers named on ransomware leak sites.

**Telegram and forum chatter**

Arabic and English posts that mention your brand, domains or executives.

HOW IT WORKS

See. Verify. Remove.

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

1 See**Collection**

Sources are collected continuously and matched against your domains, brands and people.

2 Verify**Analyst verification**

Findings are enriched, de-duplicated and confirmed by an analyst.

3 Remove**Response**

We recommend actions, such as password resets, and can remove public exposures.

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 context**

Source, date, exposed data and recommended action for every finding.

**Credential exposure reports**

Which accounts are exposed and which need reset first.

**Dashboards and reports**

Exposure 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