

Attack Surface Monitoring | Platform module

See your organization the way attackers do.

Cybersee discovers the internet-facing assets linked to your organization, including the ones nobody remembers, and flags the exposures attackers look for first.

Asset inventory, acme.sa

21 assets · 27 services

vpn.acme.sa	443	Fortinet FortiGate	Critical
remote.acme.sa	3389	Remote desktop	High
old.acme.sa	80	Grafana, no login	High
dev.acme.sa	8443	Jenkins	Medium
www.acme.sa	443	nginx 1.24	Low

WHY IT MATTERS

What you get with Attack Surface Monitoring



Find forgotten assets

Old subdomains, test servers and third-party hosted systems are discovered automatically.



Fix what matters first

Issues are prioritized by risk, with known exploited vulnerabilities at the top.



Stay continuously current

New assets and changes are detected as they appear, not once a year.

WHERE WE LOOK

DNS records

Certificate transparency logs

Internet-wide scan data

Public banners

Cloud provider ranges

WHOIS and registrar data

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 Attack Surface Monitoring detects



Unknown subdomains and hosts

Assets discovered from DNS, certificates and internet scan data.



Exposed remote access

RDP, SSH, VPN and management ports reachable from the internet.



Unprotected admin panels

Dashboards and consoles exposed without authentication.



Outdated technology

Software versions with known vulnerabilities, including actively exploited ones.



Certificate issues

Expired, expiring and misconfigured TLS certificates.



Email and DNS security

Missing or weak SPF, DKIM and DMARC records.

HOW IT WORKS

See. Verify. Remove.

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

1 See

Discovery

Assets linked to your domains are discovered passively and mapped continuously.

2 Verify

Validation

Exposures are checked, prioritized by risk and confirmed by an analyst.

3 Remove

Remediation

Clear fixes are sent to your team and tracked until resolved.

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

**Living asset inventory**

Every internet-facing asset with IP, ports, technology and owner.

**Prioritized issues**

Risk-ranked findings with a recommended fix for each.

**Dashboards and reports**

Exposure trends and monthly reports for management.

**Integrations and API**

Issues pushed to your ticketing and SIEM 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