CYBERMON

ATTACK SURFACE INTELLIGENCE

You have deployed more to the internet than you can account for.

So has everyone. Attackers count on it.

CyberMon ASI discovers everything your organisation exposes to the internet — continuously, from the outside in, the same way an attacker would — and returns a prioritised list with the evidence attached.

YOU ALREADY KNOW THE SHAPE OF THIS PROBLEM

A campaign subdomain from two years ago, still resolving.

An AI endpoint published last month, on no asset register.

A login page exposed with no MFA visible from outside.

An admin interface with a certificate that expired months ago.

None of it is on your inventory spreadsheet. All of it is on the internet.

HOW AN ASSET NOBODY LISTED BECOMES A FINDING

You give us	→	Attribution finds	→	Resolves to	→	Running	→	Finding
`example-corp.com`		An unlisted host		An attributed IP		An expired-cert admin panel		Exposed admin interface, unlisted host

Illustrative — invented data. Not a customer finding, and not a redacted one.

ASSETS DISCOVERED

Domains · IP addresses · APIs · Cloud resources · Shadow IT

WHAT IS THEN CHECKED

CVE detection · Web vulnerability detection · TLS / SSL posture · Weak configuration checks · AI & LLM endpoint exposure · Login / MFA detection

START HERE — NO COST, NO COMMITMENT

Get a free leak-and-exposure report

The fastest way to find out whether this is your problem too.

cybermon.co.in

Free report · live platform

TALK TO US

reachus@cybermon.co.in

+91 94836 47986 · www.cybermon.co.in

Bengaluru, India

TARGET SECTORS

Technology & SaaS · BFSI · Healthcare · Energy & Infrastructure · Government & Telecom · Retail & E-commerce

ASI is one of three CyberMon products. Digital Risk Intelligence and Compliance & Cloud Security correlate with it into a single prioritised risk score.