CYBERMON

PRODUCT COVERAGE DOCUMENT

Digital Risk Intelligence

Detect. Prioritize. Respond.

What DRI is

Digital Risk Intelligence looks at **what is being said, sold and faked about you outside your firewall** — on leak sites, in dark web forums, on Telegram, in app stores and on social media.

These are places your security controls cannot reach and your logs will never show you. A credential stolen from an employee's personal device by information-stealer malware does not trigger an alert on your network. It appears in a stealer log, gets traded, and is used weeks or months later. A cloned mobile app in a third-party store harms your customers without ever touching your infrastructure. A ransomware group listing your supplier on a leak site is your problem before it is anyone's incident.

CyberMon DRI monitors those channels continuously, attributes what it finds to your organisation, and converts it into an alert an analyst can act on.

> *"We watch what's being sold about you. If your employee's credentials are in a stealer log tonight, you know tomorrow — not in two hundred and sixty-three days."*
>
> CYBERMON DRI — POSITIONING

Sources monitored

DRI collection runs across nine classes of external source. Each is normalised into a common format before analysis, so a credential found on a paste site and one found in a Telegram channel are assessed the same way.

Data leak sites

Sites where stolen corporate data is published or advertised.

Dark Web Forums

Access-sale and database-sale chatter on the dark web.

Carding Forums

Marketplaces trading stolen credit and debit card data.

Paste Sites & Public Code Repositories

Public paste services and code repositories where dumped data and credentials surface first.

Credential Leaks

Combolists, breach dumps and stealer-log output containing corporate accounts.

Phishing Infrastructure

Impersonating domains and hosting used to target your customers and staff, including country-code (ccTLD) domains.

App Stores

Google Play, the Apple App Store, and third-party app stores.

Social Media Impersonation

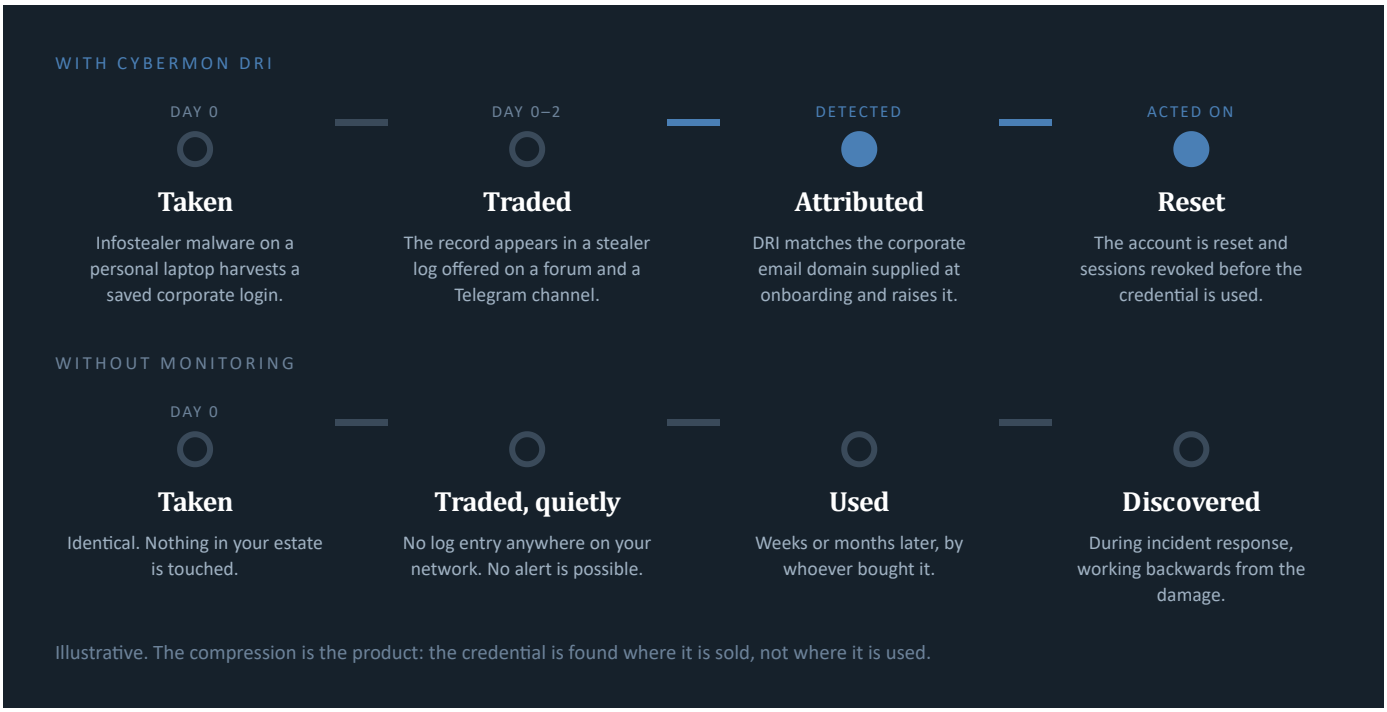
Fake handles, pages and groups on Facebook, X and LinkedIn.

Telegram Channels

High-value channels used to trade access, data and credentials.

"Every finding is deduplicated, scored, and converted into an actionable alert."

The 263-day gap, closed



Core capabilities

Nine named capabilities make up the product.

Data Leak Monitoring

Company data, documents and trade secrets appearing outside your control — on leak sites, in dumps and in paste services.

Credential Exposure

Corporate email and credential exposure monitoring, including credentials harvested by information-stealer malware and traded in stealer logs.

Ransomware Intelligence

Victim listings and actor disclosures — including mentions of your organisation, your subsidiaries, or your suppliers.

Social Media Intelligence

Fake social media handles, posts and groups, including impersonation of named executives.

Dark Web Forums

Access-sale and database-sale chatter — the market in which initial access to an organisation is bought before it is used.

Fake Apps

Applications impersonating your brand on Google Play, the App Store and third-party app stores.

Phishing Website

Impersonating URLs, typosquat domains and phishing kits built to target your customers, staff or brand.

Stolen Credit/Debit Card Information

Compromised card numbers, CVV and cardholder data offered for sale on carding forums and dark web marketplaces.

Takedowns

Take down of impersonating domains, social media handles, apps and other content from the open web.

Detection surfaces — what is actually looked for

SURFACE	WHAT DRI DETECTS
Corporate data	Company data, documents and trade secrets published, leaked or advertised for sale.
Credentials	Corporate email addresses and credentials in stealer-log output, breach dumps and combolists.
Ransomware exposure	Victim listings and threat-actor disclosures naming your organisation or entities connected to it.
Domain impersonation	Typosquat domains, impersonating URLs and the phishing kits deployed on them, including country-code domains.
App impersonation	Fake and cloned applications on Google Play, the Apple App Store and third-party app stores.
Brand and executive impersonation	Fake social handles, pages, groups and posts on Facebook, X and LinkedIn, including impersonation of named executives.
Access brokerage	Access-sale and database-sale chatter naming your organisation on dark web forums and Telegram channels.
Stolen credit/debit card data	Compromised card numbers and cardholder data offered for sale on carding forums, matched against your issued card ranges where supplied.

A worked example: the app that was not yours

Invented, and typical of what brand monitoring surfaces. Names are fictional.

1. **What appeared.** An application called “Example Corp Rewards” published on a third-party Android store, using the brand’s name, icon and colour scheme. It requested contacts and SMS permissions the genuine app does not.
2. **What DRI matched.** The brand name and icon against the app-store listing, and a typosquat domain `example-corp-rewards.example` used as the listing’s support URL — which was also hosting a phishing page imitating the customer’s login.
3. **What was in the alert.** The listing, the developer account, screenshots, the permissions requested, the domain registration detail and the phishing page — captured as evidence rather than described.
4. **What happened next.** CyberMon analysts filed the takedown for the listing and the domain. Takedowns are an analyst-led service; volume and turnaround are scoped in the agreement, and no platform guarantees removal.

The point: none of this touched the customer’s infrastructure. It harmed their customers, under their brand, in a place their security tooling does not look.

Key features

FEATURE	WHAT IT MEANS IN PRACTICE
Deduplicated, scored alerts	Every finding is deduplicated, scored, and converted into an actionable alert. The same leaked record surfacing across four sources is one alert.
Evidence attached	Every finding ships with proof — the record, the screenshot, the config. Directly usable for incident response, board reporting and DPDP breach notification.
India-weighted collection	Coverage of app stores, regional phishing infrastructure and Telegram channels that global vendors under-index on.
Built for small security teams	Deduplication and scoring built for teams of two to ten, not a 40-analyst SOC. The output is an action, not a feed.
Correlation with exposed assets	A leaked credential is joined to the exposed asset it opens and the compliance control that covers it, rather than arriving as an isolated alert.

Takedowns

DRI includes takedown of impersonating domains, social media handles, apps and other content from the open web.

Please note the scope precisely

Takedowns are delivered as an **analyst-led service**. CyberMon does not currently offer an automated takedown workflow, and nothing in this document should be read as committing to one. This distinction is contractual, not cosmetic.

What customers gain

Early Warning

Surface threats before they escalate into incidents.

Faster Detection

Reduce time-to-discovery on leaked credentials and data.

Reduced Brand Abuse

Identify and act on impersonation before customers are harmed.

Better Visibility

Continuous view of external threat activity targeting your organisation.

Prioritized Alerts

Less raw noise — only what needs your attention.

Stronger Readiness

Evidence-backed preparation for incident response and compliance.

Who DRI is for, and the problem it solves

Target sectors: BFSI · Healthcare · Energy & Infrastructure · Government & Telecom · Retail & E-commerce · Technology & SaaS.

BUYER	THE PROBLEM DRI IS BOUGHT TO SOLVE
BFSI	Customers targeted by phishing domains and fake banking apps; staff credentials traded in stealer logs; regulatory expectation of external threat visibility and evidence.
E-commerce & retail	Cloned storefronts, fake apps in third-party stores, and impersonating social accounts running promotions in your name.
Technology & SaaS	Source code and customer data in leak channels; access to your tenant advertised on dark web forums before it is used.
Healthcare	Patient data appearing on leak sites; ransomware groups listing you or a connected provider.
Government suppliers	Demonstrable external monitoring as a condition of supply; early notice when a connected entity is breached.

The questions DRI is bought to answer

- Are any of our corporate credentials for sale right now?
- Is anyone impersonating our brand, our app or our executives to our customers?
- Has a ransomware group listed us — or one of our suppliers?
- Is our data on a leak site, and can we prove what was in it?
- If a regulator asks tomorrow what we knew and when, can we show them?

What you need in place to get value from this

Someone who can act on a finding. CyberMon finds, prioritises and evidences; it does not remediate. A finding lands with the person who owns the affected asset — a sysadmin, a cloud or platform engineer, a security lead. That can be one part-time person, and it does not need to be a security specialist, but it cannot be nobody.

Someone to receive the alerts, and **authority to change what is found.** If the exposed asset belongs to a team that will not act on it, the finding does not become a fix.

Delivery

What is built and running today

- **Automated asset discovery and ingestion pipelines** across all three products.
- **Risk scoring, deduplication and correlation engine** in production.
- **Threat-source normalisation** across leak sites, forums, paste sites and app stores.
- **Analyst alert queue, evidence capture and customer reporting workflow.**
- **Live platform at cybermon.co.in**, including free leak-and-exposure reporting.

Onboarding & reporting

Onboarding establishes the monitoring profile — the brands, domains, executives and corporate email domains to be attributed to your organisation — after which collection and normalisation run on an ongoing schedule across the nine source classes. Findings reach you through the analyst alert queue and the customer reporting workflow, every one carrying its proof. Reporting cadence, alert channel and the notification target for a critical finding are agreed at scoping.

How it is bought

Digital Risk Intelligence is sold as an annual subscription, scoped per engagement against the customer's attack surface, exposure level and industry. Pricing is quoted per engagement — speak to CyberMon, or to your CyberMon partner, for a scoped quote. Takedown volume and terms are scoped separately; see the note under *Takedowns*.

CyberMon DRI

Detect. Prioritize. Respond.

CyberMon LLP · Bengaluru, India · LLPIN ACZ-2481 · cybermon.co.in

Free leak-and-exposure reporting is available on the live platform.