Some of Your Data Is Already Out There.

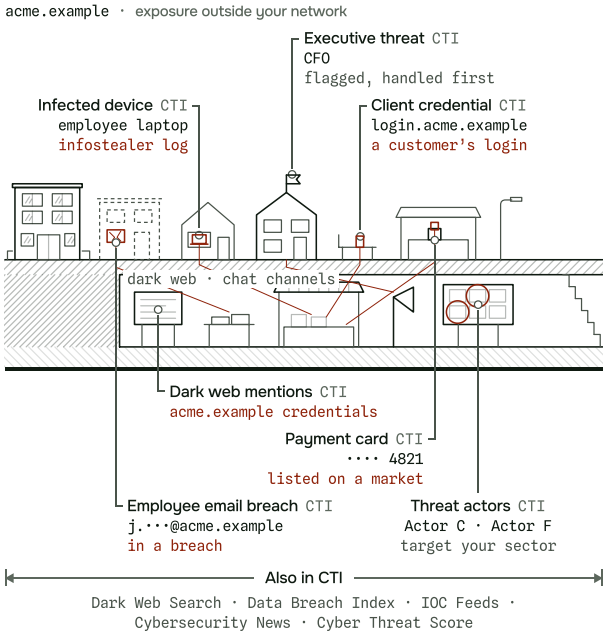
Cyber Threat Intelligence reads breach data, infostealer logs and dark web sources for your domains, your employees and your customers, and profiles the threat actors aimed at your sector.

CYBER THREAT INTELLIGENCE

Some of Your Data Is Already Out There.

Cyber Threat Intelligence reads breach data, infostealer logs and dark web sources for your domains, your employees and your customers, and profiles the threat actors aimed at your sector.

Every exposure is tied to something your team can act on: an account, a device, a credential or a card.



Exposure That Never Touches Your Network.

Your logs record what happens inside the perimeter. The exposures CTI finds happened somewhere else: in another company's breach, on a device you don't manage, in a market your tools never see.

OTHER BREACHES

A Service Your Staff Signed Up For

When a third party is breached, the corporate addresses registered there leak with whatever was stored beside them. A reused password turns their breach into yours.

UNMANAGED DEVICES

A Laptop Outside Your Fleet

An infostealer on a personal or contractor machine takes the browser's saved logins, cookies and autofill data, including the entries for your SSO and VPN.

CLOSED VENUES

Forums, Markets and Leak Sites

Stolen data and access change hands in places search engines don't index. Nobody sends the victim a notice.

Monitoring and Context in One Picture.

The monitoring capabilities match breaches, stealer logs and leaked credentials to your domains. Threat actor profiles and news supply the context.

Monitoring

breaches, stealer logs and leaked credentials, matched to your domains

Dark Web Mentions Monitoring

A NAME OR DOMAIN

Your organization's names and domains, watched on dark web sources instead of searched by hand.

Employee Email Breach Monitoring

AN ACCOUNT

Corporate addresses in known breaches, and the data types that leaked with them.

Compromised Employee Device Monitoring

A DEVICE

Infostealer infections on devices that hold your employees' credentials.

Compromised Client Credential Monitoring

A CREDENTIAL

Your customers' leaked logins for your services, each tracked through a state.

Compromised Payment Credential Monitoring

A CARD

Leaked payment cards linked to your organization, worked through the same states.

Executive Threat Monitoring

A PERSON

Executives and VIPs flagged, so the exposures that touch leadership are handled first.

Context

threat actor profiles and news

Threat Actor Intelligence

AN ACTOR

Origin countries, targeted regions, industries and organizations, and the CVEs and tools each actor uses.

Cybersecurity News

A STORY

Curated news, each item linked to the CVEs, threat actors and issue types it concerns.

ALSO IN CTI

Dark Web Search
the same sources, queried by text or indicator

Data Breach Index
the catalog of breaches behind the monitoring

IOC Feeds
indicators, packaged for detection and blocking

Cyber Threat Score
the scoring layer across the Deepinfo Platform

Each Finding Arrives Tied to an Account, a Device or a Person.

CTI keeps findings as structured records, not headlines. Each record points at an account, a device, a credential or an actor, and each one is searchable under `/v1/cti/` in the API.

BREACHED ACCOUNT	The corporate address, the breaches it appears in, and the profile fields your team sets: VIP flag, name, title
BREACH	Date, description, the data types exposed and the number of your accounts affected
COMPROMISED DEVICE	Hardware ID, user and system info, password, token, autofill, cookie and sensitive-cookie counts, same-password rate
LEAKED CREDENTIAL	An employee login, a customer login for your services or a payment card, each with the state your team has set

THREAT ACTOR	Identity and profile, origin countries, activity across leaks, forums and markets, targets, and the CVEs and tools used
NEWS ITEM	The story, linked to the CVEs, threat actors and issue types it concerns

Compromised devices, employee credentials and threat actors each have their own search, using the platform's filter syntax.

From Leaked Credential to Closed Finding.

Closing a credential finding doesn't delete it. Each one carries a state, so the next analyst can see what was decided and revert it if the call was wrong.

01 → 02 → 03 → 04

Collect

Deepinfo collects breach data, infostealer logs and dark web content, and indexes each record for search.

Match

Records are matched to your domains and services, so each finding lands on an address, a device, a credential or a card.

Decide

Your team marks a credential resolved, accepts the risk, ignores it or marks it a false positive, one at a time or by filter. Revert restores the previous state.

Report

New email breaches trigger a notification at the frequency you choose, from instant to monthly. The CTI Email Breach Summary is a PDF report, on demand or on a schedule.

Know Which Actors Target Organizations Like Yours.

Each profile records who the actor is (size, types, sophistication and specializations), where it comes from, which leaks, forums and markets it shows up in, and whom it targets, down to regions, countries, industries and organizations.

Capabilities are recorded too: the CVEs and the tools the actor uses. Filter by industry to see who is aimed at your sector, then check those CVEs against what External Attack Surface Management finds on your assets.

MOST TARGETED Countries, industries, organizations	MOST USED CVEs and tools
ACTOR ORIGIN Countries hosting the most actors	SEARCH By target, CVE or tool

Query This Data Through the API

Credentials and dark web findings stay in the Deepinfo Platform. The domain and vulnerability data around them is open through the API. The index holds 400M+ domains, 2B+ subdomains, 200B+ DNS records and 30B+ SSL certificates.

Vulnerability Search API API →	Domain Detail API API →
Vulnerability Detail API API →	WHOIS History API API →

See Your Own Exposure, From the Outside.

REQUEST A DEMO

www.deepinfo.com/request-demo

PRICING

www.deepinfo.com/pricing

API DOCUMENTATION

docs.deepinfo.com

OFFICES

Istanbul (HQ)
Paris
Kuwait City

CONTACT

www.deepinfo.com/contact

SECURITY

security@deepinfo.com

© 2026 DEEPINFO