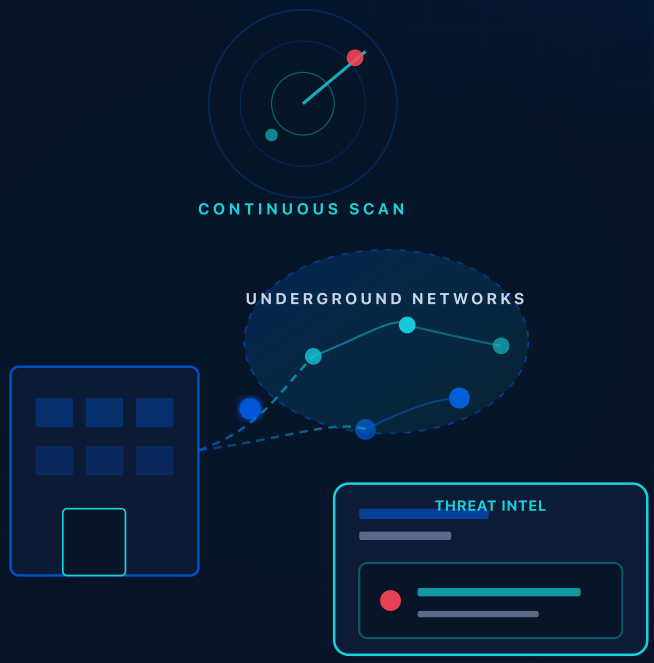
DARK WEB MONITORING

What's Being Said About You in the Shadows?

Your credentials, data, intellectual property, and brand may already be circulating across criminal forums, breach databases, and underground marketplaces.

> Suzu Labs Dark Web Monitoring finds leaked credentials, data, and brand abuse before criminals use them against you.



24/7	50K+	<4hr	100%
MONITORING	SOURCES TRACKED	ANALYST OUTREACH	HUMAN VERIFIED

THE PROBLEM

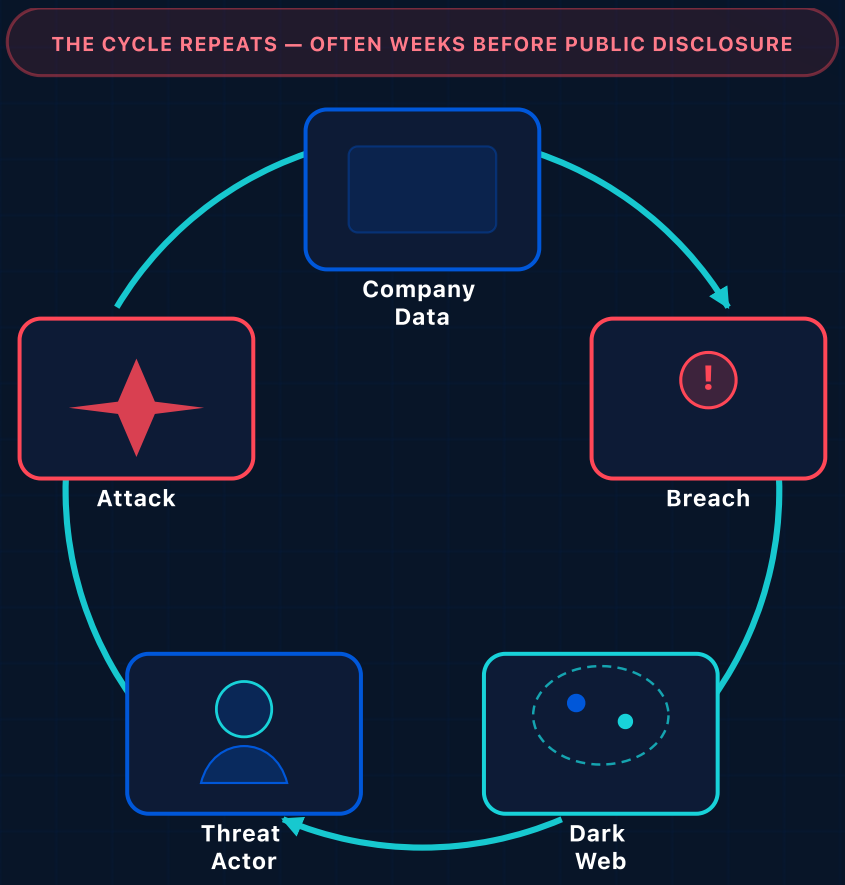
You Can't Protect What You Can't See

Most organizations focus on securing internal systems while attackers collaborate openly in places most companies never monitor.

Threat actors routinely exchange:

Stolen credentials	Corporate email accounts	Customer records	Source code
Internal documents	Executive information	Vulnerability intelligence	Attack planning data

Often, organizations don't learn about exposure until long after attackers do.



> *"By the time a breach becomes public, criminals have often been discussing it for weeks or months."*

WHAT WE MONITOR

Dark Web Monitoring Coverage

We scan criminal forums, marketplaces, breach dumps, and encrypted channels for mentions of your company, people, and assets.

Credential Exposure

Alerts when employee or customer credentials show up in breaches, paste sites, or criminal marketplaces.

- Employee email and password pairs
- VPN, SSO, and admin login leaks

Brand Impersonation

Phishing kits, fraudulent domains, fake brands, and criminal campaigns that target your company.

- Lookalike domains and fake login pages
- Phishing kits using your brand assets

Vulnerability Intelligence

Exploits being developed, sold, or discussed in criminal channels before they hit the news.

- Exploit sales ahead of public patches
- Zero-day discussion in criminal forums

Data Leaks

Proprietary data, internal documents, customer information, and source code posted where it should not be.

- Internal documents and customer records
- Source code, API keys, and configs

Targeted Threats

Forum discussions, attack planning, and posts tied to your company, industry, or leadership team.

- Attack planning against your organization
- Industry and leadership-specific chatter

Forum Monitoring

Forum and channel posts that mention your company, executives, infrastructure, or vendors.

- Executive and company name mentions
- Infrastructure and vendor references

OUR PROCESS

From Collection to Action

Our analysts collect intelligence from the dark web, verify what matters, and reach out with findings your team can use. No noise, no guesswork.

STEP 1

Collection

Our analysts collect data from over 50,000 dark web sources, including forums, marketplaces, breach dumps, and encrypted channels. Monitoring runs continuously so new exposure is not waiting on a scheduled scan.

50,000+ SOURCES

STEP 2

Analysis

Analysts confirm what is real and what matters to your organization. Duplicate listings, stale credentials, and unrelated chatter are filtered out before anything reaches your team.

ANALYST VERIFICATION

STEP 3

Analyst Outreach

An analyst reaches out with context, a risk rating, and suggested next steps. You hear from a person who can answer questions, not an automated alert or ticket queue.

<4 HOUR DELIVERY

STEP 4

Response

Our team supports investigation, takedowns, credential resets, and ongoing threat monitoring. We stay involved through remediation so exposure does not reopen quietly.

REMEDIATION SUPPORT

WHO BENEFITS

Industries We Serve

Firewalls, EDR, and SIEM cover your network. Dark web monitoring covers what leaks out and gets traded elsewhere.

Financial Services

ATO
WIRE FRAUD

Protect customer accounts, SWIFT access, and employee credentials traded on fraud forums before wire fraud campaigns launch.

EXAMPLE

Loan officer VPN credentials with active banking sessions appear on a fraud marketplace. Your team is alerted before wire fraud begins.

Healthcare

HIPAA
RANSOMWARE

Detect patient records, insurance IDs, and clinician credentials on criminal channels. Lowers breach notification costs and compliance risk.

EXAMPLE

12,000 patient records listed on an underground marketplace, traced to a misconfigured vendor. Found weeks before disclosure.

Technology

IP THEFT
SUPPLY CHAIN

Catch source code dumps, API keys, and developer credentials before they're used in supply chain or zero-day attacks.

EXAMPLE

Production AWS keys and repo credentials posted to a paste site after a phishing incident. Contained before data access.

Gov Contractors

CUI
CMMC

Find controlled documents and cleared employee credentials posted outside authorized systems. Supports CMMC and DFARS requirements.

EXAMPLE

Proposal documents and credentials found in a ransomware leak catalog. Takedown began before public release.

Executive Leadership

BEC
TARGETING

Track doxxing, personal credential leaks, and impersonation campaigns built around C-suite and board member profiles.

EXAMPLE

CFO email in a combo list alongside forum posts planning wire fraud. Security and legal notified within hours.

Hospitality & Gaming

PII
BRAND ABUSE

Find loyalty program credentials, payment data, and fake booking sites targeting your guests before fraud and brand abuse spread.

EXAMPLE

Clone booking site on a phishing marketplace with 3,200 guest credentials. Takedown started before the campaign scaled.

Dark web monitoring finds problems your other tools miss.
It gives your team time to respond before criminals act.

NEXT STEP

What Would You Find If You Looked Today?

Most organizations have never examined their dark web exposure.

Our team runs a complimentary assessment to find risks tied to your domain, employees, credentials, and public-facing assets.

No software to install. No agents on your network.
We run the assessment and walk you through what we find.

ASSESSMENT INCLUDES

- ✓ Credential Exposure Review
- ✓ Breach Intelligence Snapshot
- ✓ Brand Abuse Analysis
- ✓ Threat Actor Discussion Review
- ✓ Executive Exposure Assessment
- ✓ Review of Findings with Our Team

ABOUT SUZU LABS

Suzu Labs is a cybersecurity firm run by practitioners: threat intelligence analysts, red teamers, and offensive security operators. The same team that monitors the dark web can test your systems, respond to incidents, and help you meet compliance requirements.

WHAT ELSE WE DO

- → Penetration testing & CAO
- → Privacy engineering
- → Governance, risk & compliance
- → Incident response & forensics
- → AI security advisory
- → Exposure & vulnerability management

Suzu Labs

THREAT INTELLIGENCE · OFFENSIVE SECURITY · AI SECURITY · SUZULABS.COM