

Dark web intelligence.

See what the cyber underground knows about your organization, and act on it before attackers do.



— OVERVIEW

Why it matters.

Stolen credentials, leaked customer records and lookalike domains usually show up on the dark web before anyone uses them against you. Seeing them there first buys your team time.

StrikeReady Dark Web Intelligence watches underground forums and marketplaces in near real time. When something about your company appears, it lands in the SOC as a case with the evidence attached.

So when a ransomware crew names you or someone clones your login page, your analysts hear about it early and **act on it from the same console.**

How StrikeReady Dark Web Intelligence works

01

Collect

StrikeReady scans the dark web around the clock and pulls out anything that points back to you.

02

Prioritize

Each finding is ranked by its impact and by which of your assets it touches.

03

Alert

Configurable alerts send critical findings to the people who own them.

04

Act

Findings flow into SOC workflows for validation, response and reporting. Impersonating domains go straight to takedown.

CAPABILITIES

Key features.

Ranked findings from the underground economy, ready for your SOC to work the same day.



Real-time dark web scanning

Monitors dark web forums, marketplaces and hidden communication channels for exposed company data, stolen credentials and signs of malicious activity aimed at you.



Data leak detection and blast radius

Flags leaked credentials, financial records, trade secrets, intellectual property and personal data (PII), and shows how far the exposure reaches so you can contain it.



Threat intelligence inside your SOC

Dark web findings feed the threat intelligence your SOC already uses, so analysts see underground activity next to every other signal when they make a call.



Custom alerting

Build alerts around keywords, specific assets or named employees, and route each one to whoever needs to act on it.



Domain takedown

Detects lookalike, phishing and typosquat domains impersonating your brand, and lets analysts request a takedown directly from StrikeReady. StrikeReady files the request with the domain's registrar or hosting provider and tracks it through to resolution, so nobody's raising tickets by hand or chasing hosting portals.



Entity-based monitoring

Track the assets attackers go after, everywhere they come up in the underground.

Domains

Your websites and affiliated domains, plus lookalikes registered to impersonate them.

Executives

C-suite and high-profile staff whose data gets used in targeted attacks.

CVEs

Vulnerabilities under discussion that could hit your systems.

IP and MAC addresses

Your network addresses, watched for signs of unauthorized access.

— IN THE FIELD

Use case scenarios.

8 ways security teams use dark web intelligence day to day.

**SCENARIO 01****Credential compromise detection**

An employee's credentials go up for sale on a dark web marketplace. StrikeReady alerts right away, so the team can reset the password, tighten monitoring on the account and trace where the breach started.

**SCENARIO 02****Credential leaks matched to identity systems**

StrikeReady matches leaked credentials against Entra ID, Active Directory, Google IAM and Okta. Analysts see every related alert, dark web sources included, and get the full picture of where and how a user was exposed.

**SCENARIO 03****Automatic case creation for leaked data**

When leaked credentials are found, StrikeReady opens a case and fills in the alert sources, breach details and associated risk. The analyst starts the investigation with the paperwork already done.

**SCENARIO 04****PII exposure and response**

Customer or employee records show up in a dark web data dump. The alert gives the team what it needs to notify the people affected and close the gap that leaked them.

**SCENARIO 05****Brand and executive protection**

Executive names and company aliases come up in threat actor discussions. The security team gets an alert and puts defenses in place before a targeted phishing or impersonation attempt lands.

**SCENARIO 06****Impersonating domain takedown**

A typosquatted domain mimicking the corporate login page goes live. StrikeReady flags it and shows its screenshot and favicon next to the real brand domain, so the analyst can confirm the impersonation at a glance. One request from the case files the takedown with the registrar or hosting provider, and the case tracks it until it's resolved. Analysts can submit several domains in a single action.

**SCENARIO 07****Threat actor campaign monitoring**

StrikeReady tracks threat actors as they trade exploits and talk through vulnerabilities, so you can patch and harden your infrastructure before the attack starts.

**SCENARIO 08****IOCs fed into SOC tools**

Indicators of compromise (IOCs) found on the dark web go straight into your SOC tools for validation in real time.

— OUTCOMES

What you get.



Earlier threat detection

Spot risks while they're still being traded and discussed, before they turn into an active attack.



Less risk exposure

Act on leaked data and exposed vulnerabilities as soon as they're found.



Wide coverage

Track your domains, IPs, CVEs and executives across the dark web.



A faster SOC

Collection, prioritization and response workflows run automatically, so analysts spend their time on investigation and response.



Better decisions

Enriched intelligence shows which threats to deal with first.



Faster brand protection

Go from detecting an impersonating domain to filing its takedown without leaving the SOC console.

Built into the SOC.

StrikeReady runs dark web monitoring inside the SOC platform your analysts already work in, next to the security tools you've already bought.

A leaked password gets matched to the user in Okta or Entra ID and opened as a case with the evidence attached. A fake login page goes from flag to takedown request in that same case.



— CONTACT US

See it in action. Book a demo.

Scan the code or go to strikeready.com/request-demo.

Questions? Email info@strikeready.com.

LinkedIn [strikeready](#) · Bluesky [strikeready.com](#) · X [strike_ready](#)



BOOK A DEMO