CybelAngel

DATASHEET

ACCOUNT TAKEOVER PREVENTION

CREDENTIAL STUFFING IS A CRITICAL THREAT TO YOUR BUSINESS

Stolen credentials are the primary vector for hackers to access your corporate IT environment and launch ransomware attacks. Today, 80%[1] of hacking techniques leverage stolen or brute-forced credentials.

Strong passwords, frequent resets, and rules for third-party application authentication are the usual policies to face these threats. But how can you stop them without having the visibility on what has been exposed, and potentially compromised?

STAY ONE STEP AHEAD OF HACKERS

CybelAngel is the only digital risk protection solution that detects and manages leaked credentials preemptively, before they are compromised.

Database scanning

Detect email addresses and passwords stored on unprotected databases. Scan instances of MySQL, PostgreSQL, MongoDB, MariaDB and ElasticSearch for exposed credentials.

Web crawling

By monitoring the clear, deep & dark web in real time, identify newly compromised credentials being shared or sold, instantly.

KEY FEATURES

10B	exposed email addresses & passwords in CybelAngel's data lake.
335k	Deep & Dark web posts detected every day.
3,000	newly exposed databases scanned every day.

KEY BENEFITS

2	Free up 2 full time employees by relying on CybelAngel.[2]
$1.7M	Avoid the costly consequences of account takeover: $1.7M on average.[2]
197	Know about exposed credentials 197 days before they are usually detected.[3]

> CybelAngel gives us a significant time advantage. They are the only solution to report credentials leaks way before they end up for sale on the Dark Web. This has proven critical for our VIPs.
>
> Chief Information Security Officer, Insurance

[1] Verizon, Data Breach Investigations Report, 2020
[2] Ponemon, The Cost of Credential Stuffing, 2017
[3] Ponemon, Cost of a Data Breach Report, 2020

GET NOTIFIED WHEN

An unprotected internal database is exposing some of your employees’ credentials.

A threat actor is sharing or selling your company’s credentials on the dark web.

A breached third-party service leaks logins & passwords of your employees.

A VIP, C-level or Board member account has been exposed.

INTRODUCING CYBELANGEL’S CREDENTIALS WATCHLIST

Real-time feed of exposed credentials.

Contextualized credentials leaks.

Unique reports - 33% of our credentials’ alerts come from unprotected databases.

Latest detection date

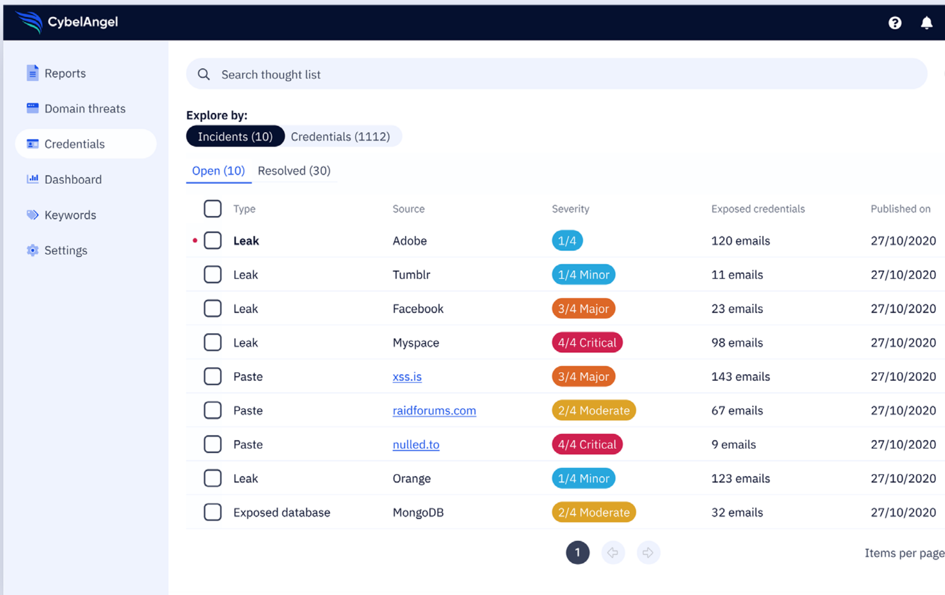
Track usernames and passwords exposed numerous times.

Confidentiality

Display or hide the passwords to your team.

Multiple views

Pivot from contextualized leak reports to exposed credential details.



Explore by:

Incidents (10) Credentials (1112)

Open (10) Resolved (30)

	Type	Source	Severity	Exposed credentials	Published on
• □	**Leak**	Adobe	1/4	120 emails	27/10/2020
□	Leak	Tumblr	1/4 Minor	11 emails	27/10/2020
□	Leak	Facebook	3/4 Major	23 emails	27/10/2020
□	Leak	Myspace	4/4 Critical	98 emails	27/10/2020
□	Paste	xss.is	3/4 Major	143 emails	27/10/2020
□	Paste	raidforums.com	2/4 Moderate	67 emails	27/10/2020
□	Paste	nulled.to	4/4 Critical	9 emails	27/10/2020
□	Leak	Orange	1/4 Minor	123 emails	27/10/2020
□	Exposed database	MongoDB	2/4 Moderate	32 emails	27/10/2020

Turn your credentials management into a seamless process

You can’t afford to manually alert every single one of your employees facing a credential leak. Integrate CybelAngel with your SOAR and SIEM and make sure you automate password changes.

Automate password resets. Connect CybelAngel with your orchestrator and reset passwords in a blink.

Educate your teams. Set up automated notifications to impacted employees and remind them of appropriate professional credentials’ use.

Update your Active Directory immediately after receiving our alerts.

Book Your Custom Demo Now

CYBELANGEL.COM

Paris | New York | London