Constella

The Identity Intelligence Playbook

A Practical Guide for CISOs and Security Teams Navigating Identity-Centric Risk

2025

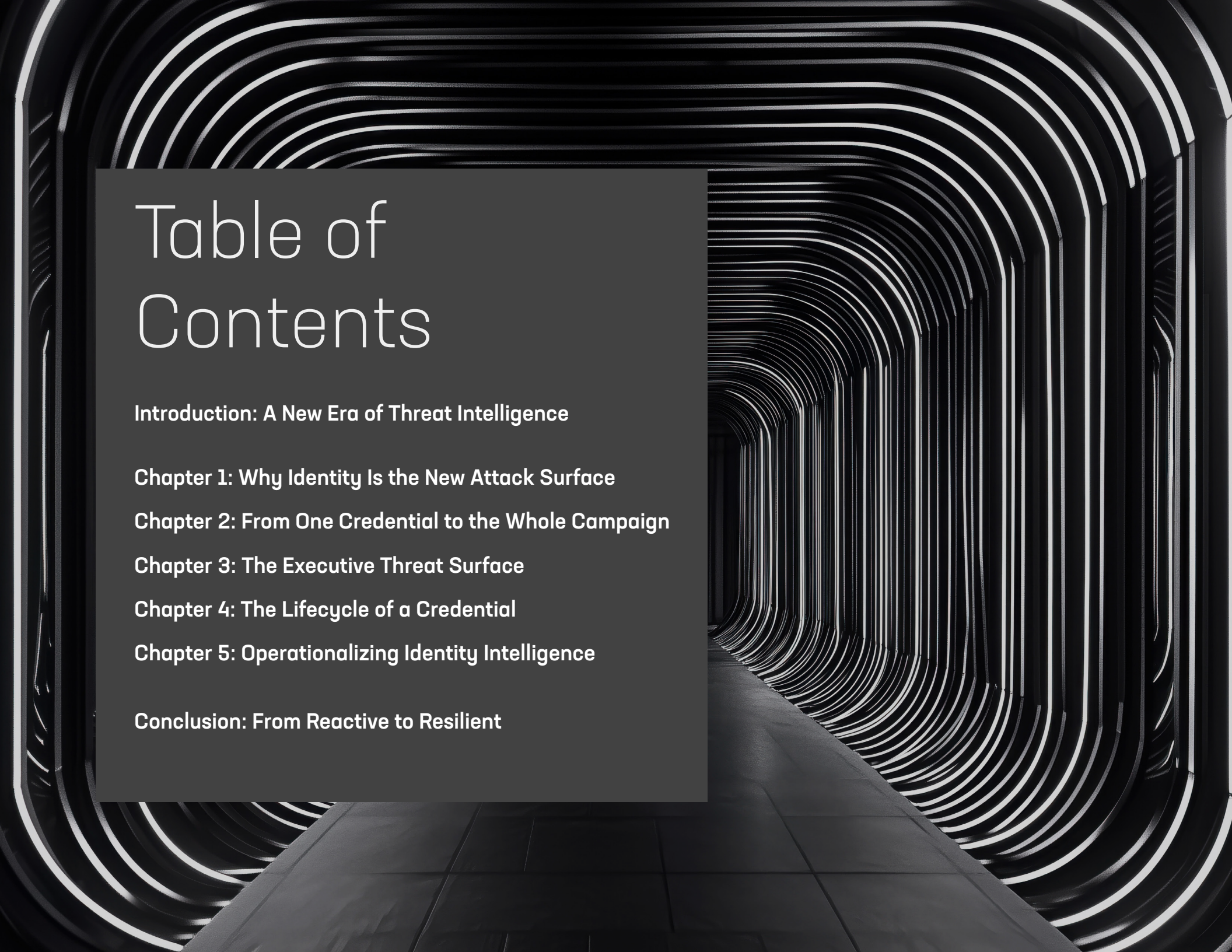


Table of Contents

Introduction:

A New Era of Threat Intelligence

For years, cybersecurity teams have depended on Indicators of Compromise (IOCs)–IP addresses, domain names, malware hashes–to detect and respond to threats. But as attackers evolve, these traditional signals are proving insufficient. Threat actors now bypass defenses by exploiting one thing defenders often overlook: identity.

> Attackers don't break in anymore – they log in. Identity is the new perimeter.

Stolen credentials, compromised session cookies, and synthetic identities have become the most valuable assets in a cybercriminal's arsenal. In fact, IBM's X-Force reported a 71% surge in the use of stolen credentials as an initial access vector in 2023. In this new threat landscape, CISOs must pivot from an IOC-centric mindset to one that prioritizes identity signals. This playbook provides a framework for using identity-centric digital risk intelligence to proactively detect, attribute, and prevent modern cyber threats.

Chapter 1:

Why Identity Is the New Attack Surface

As organizations embrace remote work, SaaS tools, and federated identity systems, traditional network perimeters have eroded. Identity has become the gateway to enterprise assets—and adversaries have taken notice.

Attackers no longer need to exploit a vulnerability or deliver malware to gain access. They log in using valid credentials, often obtained through phishing, infostealers, or breaches. The challenge? These login attempts appear legitimate to traditional defenses.

By pivoting to an identity-first approach, security teams gain visibility into:

1. Which identities are exposed in breach data.
2. Whether credentials are being sold or traded on criminal marketplaces.
3. Signs of synthetic or impersonated users.

Chapter 2:

From One Credential to the Whole Campaign

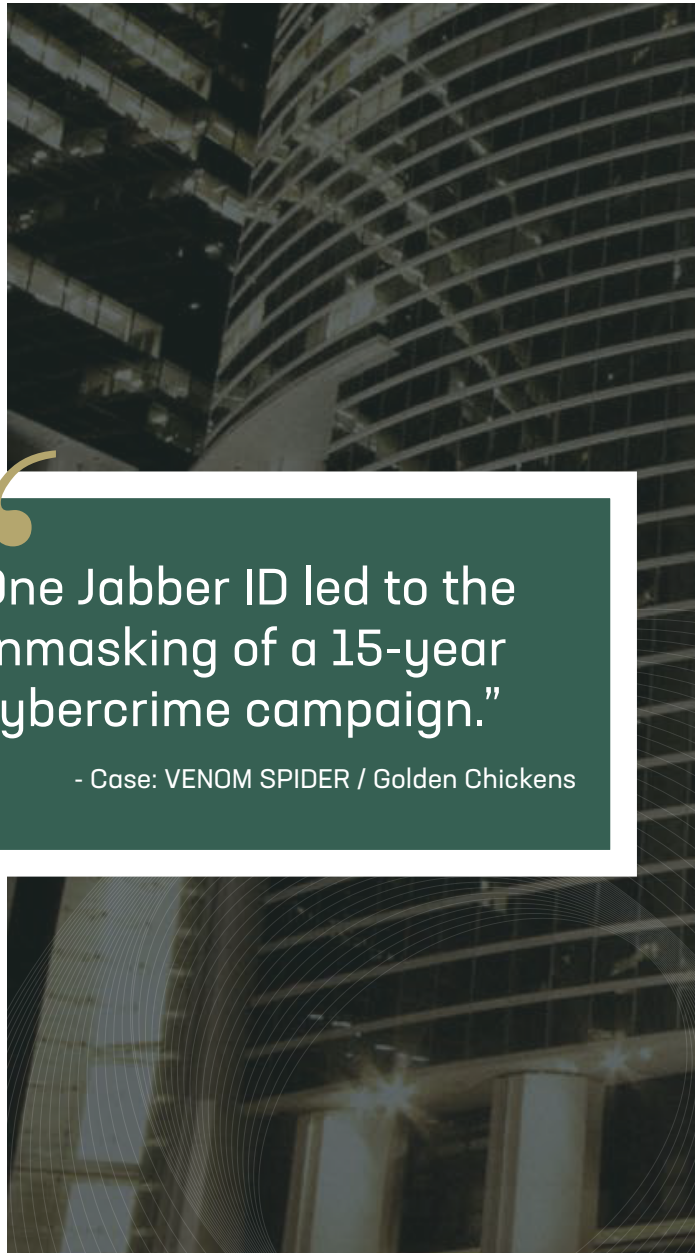
Digital risk intelligence transforms a single leaked email or password into a gateway for attribution.

Real-World Case Studies:

- A hacker known as “Jack” was unmasked after reusing a Jabber ID across forums. Pivoting on that single ID revealed over a decade of cybercrime activity.
- An infostealer log from a criminal named “La_Citrix” inadvertently exposed his own personal data, enabling full attribution.
- The takedown of AlphaBay traced back to a reused email address found in breach data.

Automated pivoting across breach records, forum posts, and malware logs enables defenders to:

- Uncover threat actor aliases and infrastructure.
- Link disparate attack campaigns.
- Surface relationships between identities, devices, and behaviorsk.



> “One Jabber ID led to the unmasking of a 15-year cybercrime campaign.”
>
> - Case: VENOM SPIDER / Golden Chickens

Chapter 3:

The Executive Threat Surface

Executives and privileged users are prime targets. Their digital footprints–across personal, corporate, and social platforms–are rich with exploitable information.

Threats include:

- Spear phishing and impersonation using leaked credentials.
- Deepfake fraud, such as AI-generated voice or video used in whaling attacks.
- Infostealer malware targeting C-level devices to harvest sensitive acces.

Notable Incidents:

- The CEO of an energy company was tricked into a wire transfer via deepfaked audio.
- Mark Zuckerberg's accounts were hijacked using a password reused from a past breach.
- Colonial Pipeline was compromised via a single leaked VPN credential.

SOLUTION: Monitoring executive identities across breach, dark web, and malware data sources to proactively identify and neutralize threats.

Chapter 4:

The Lifecycle of a Credential

Credential risk doesn't end at the breach–it evolves.

Stages of Credential Exploitation

1 Harvesting
Via phishing, infostealers, or breached systems

2 Circulation
Shared/sold on dark web, Telegram channels, or fraud marketplaces

3 Exploitation
Via credential stuffing, ATO, or access resale by initial access brokers

Limitations of Reactive Alerts:

- Often lag behind attacker activity
- Lack context (i.e., where else the credentials are in use or being discussed)

Proactive Defense

▼

Credential Pivoting + Contextual Intelligence

Security teams must move beyond "breach notifications" to:

- Pivot on exposed credentials to detect reuse and broader risk.
- Correlate breach data with malware logs, chatter, and botnet traffic.
- Identify active exploitation before damage is done.

Chapter 5:

Operationalizing Identity Intelligence

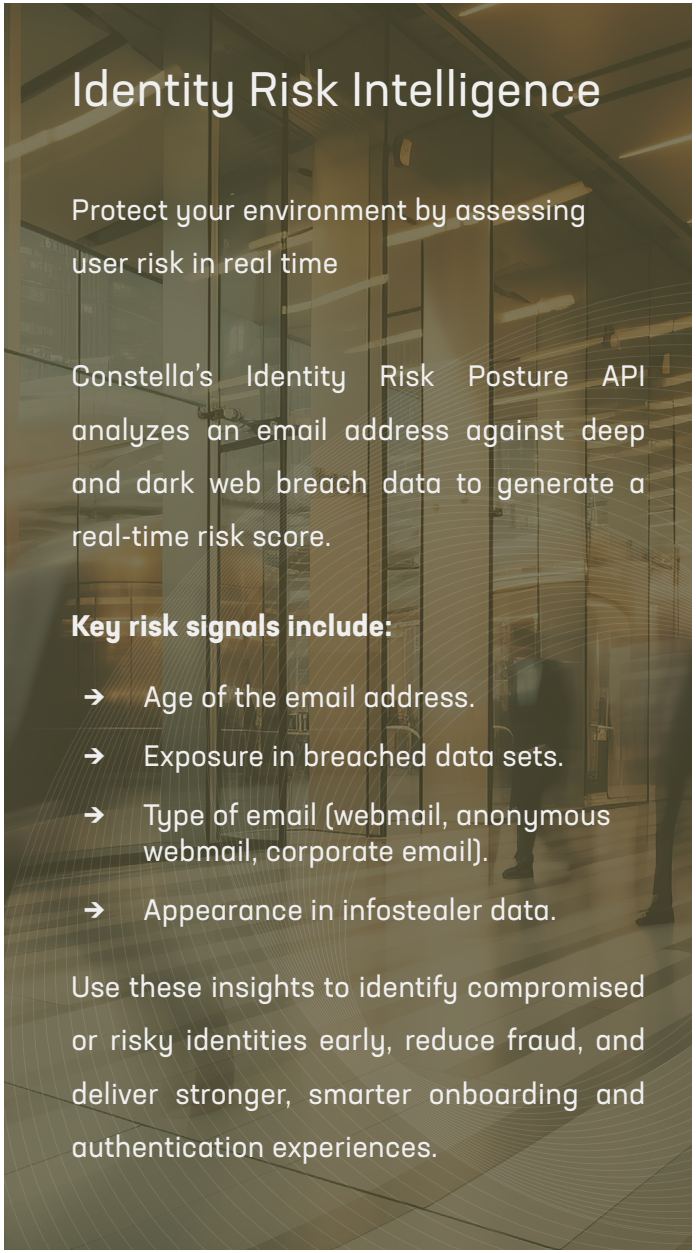
Constella Intelligence enables organizations to integrate identity-centric threat data into their existing workflows via robust APIs.

Key Capabilities:

- **Identity Risk Posture API:** Delivers a real-time score based on breach exposure, password reuse, and suspicious activity.
- **Threat Attribution Toolkit:** Enables entity graphing to map threat actor infrastructure, aliases, and campaigns.
- **Infostealer Intelligence:** Detects when a user's credentials or session cookies are being siphoned and sold.

Use Cases:

- Prioritize identity-related alerts in SIEM/SOAR.
- Flag risky identities during onboarding or access reviews.
- Monitor executive exposure in real time.



Conclusion

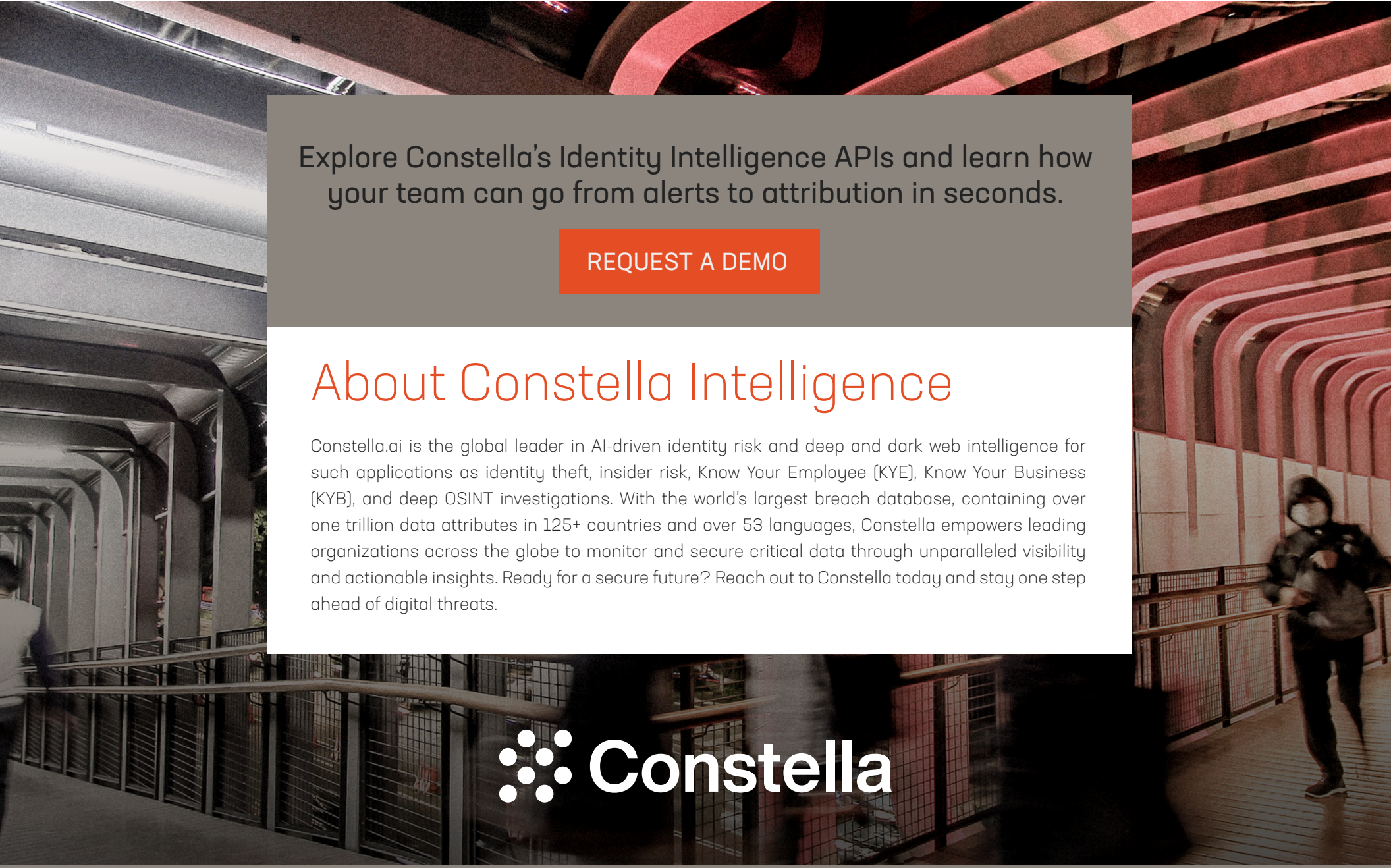
From Reactive to Resilient

In today's credential-driven attack landscape, traditional defenses fall short. Identity is now both the attack vector and the opportunity for smarter defense.

By embracing identity-centric digital risk intelligence, CISOs can:

- Detect threats earlier in the kill chain
- Attribute adversaries with greater accuracy
- Strengthen defenses around the most vulnerable users

Your Next Move: Start with a single identity. Use Constella's API to assess identity risk posture—and watch the intelligence unfold.



Explore Constella's Identity Intelligence APIs and learn how your team can go from alerts to attribution in seconds.

REQUEST A DEMO

About Constella Intelligence

Constella.ai is the global leader in AI-driven identity risk and deep and dark web intelligence for such applications as identity theft, insider risk, Know Your Employee (KYE), Know Your Business (KYB), and deep OSINT investigations. With the world's largest breach database, containing over one trillion data attributes in 125+ countries and over 53 languages, Constella empowers leading organizations across the globe to monitor and secure critical data through unparalleled visibility and actionable insights. Ready for a secure future? Reach out to Constella today and stay one step ahead of digital threats.

Constella

Visit: constella.ai **contact email : constella@constellaintelligence.com**