KODEX

Q2 2025 Threat Intelligence Report

When Criminals Built Businesses Out of Your Data

April - June 2025

Q2 2025 • Threat Intelligence Report

Table of Contents

The New Reality: Crime Goes Corporate

Threat actors didn't just infiltrate law enforcement emails in Q2 2025—**they built entire businesses around them.**

What started as opportunistic hacks has evolved into a thriving criminal economy where your users' personal information is the product, Emergency Data Requests (EDRs) are the weapon, and "doxxing-as-a-service" is the business model generating millions in revenue.

The stakes couldn't be higher. In Rio de Janeiro, compromised police credentials nearly enabled a terrorist attack at a Lady Gaga concert with 2.5 million attendees. In the United States, multiple fraudulent emergency requests from a single compromised law enforcement email enabled stalkers to discover an OnlyFans creator's real address. Across the dark web, criminals openly advertise law enforcement email access from 25+ countries for $20-1500 per account.

This isn't about theoretical vulnerabilities anymore. **This is about organized crime that's found a profitable, scalable way to weaponize your trust in data requests.**

This quarterly threat intelligence report from Kodex draws on our unique visibility across both law enforcement agencies and the world's largest companies. With a network spanning 90,000+ verified law enforcement users worldwide, Kodex has identified critical patterns in fraudulent request attempts that individual organizations typically cannot detect on their own. The insights in this report combine technical indicators with behavioral patterns to provide a comprehensive picture of this growing threat landscape.

Here's how the threat evolved in Q2—and how organizations like yours are fighting back.

Q2 Threat Trends: Three Game-Changing Developments

1. Doxxing-as-a-Service Is On the Rise

On the Rise: Criminals now advertise comprehensive doxxing services that specifically use Emergency Data Requests to extract personal information from major platforms.

“Doxxing” refers to the malicious practice of researching and publishing private information about individuals—full names, home addresses, phone numbers, email addresses, and even family member details—across public platforms with the intent to cause harm, harassment, or intimidation. What makes the current threat landscape so concerning is that criminals have weaponized legitimate law enforcement processes to obtain this sensitive data directly from the platforms where users thought it was secure.

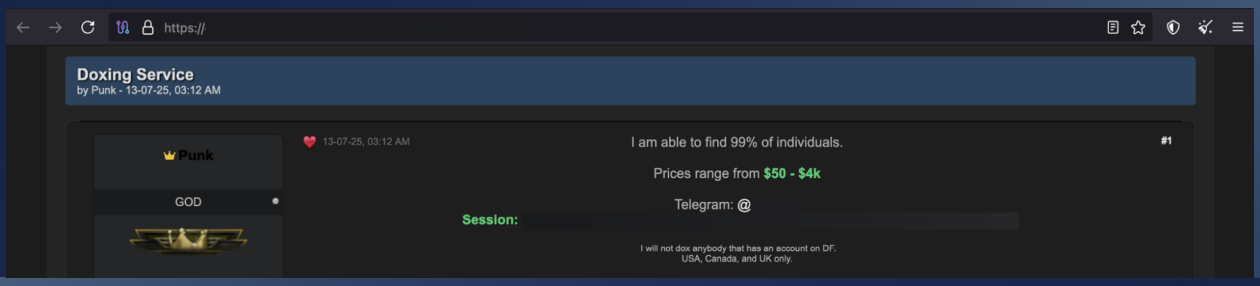
The process works with devastating efficiency: Threat actors either compromise authentic law enforcement email accounts or create convincing fake domains that closely mimic legitimate police departments. They then submit urgent Emergency Data Requests to major social media platforms, claiming they’re investigating child safety emergencies or situations where “an individual would suffer greatly or die” without immediate data access. These platforms, operating under intense time pressure and legal obligations to assist law enforcement, often release user data without thorough verification.

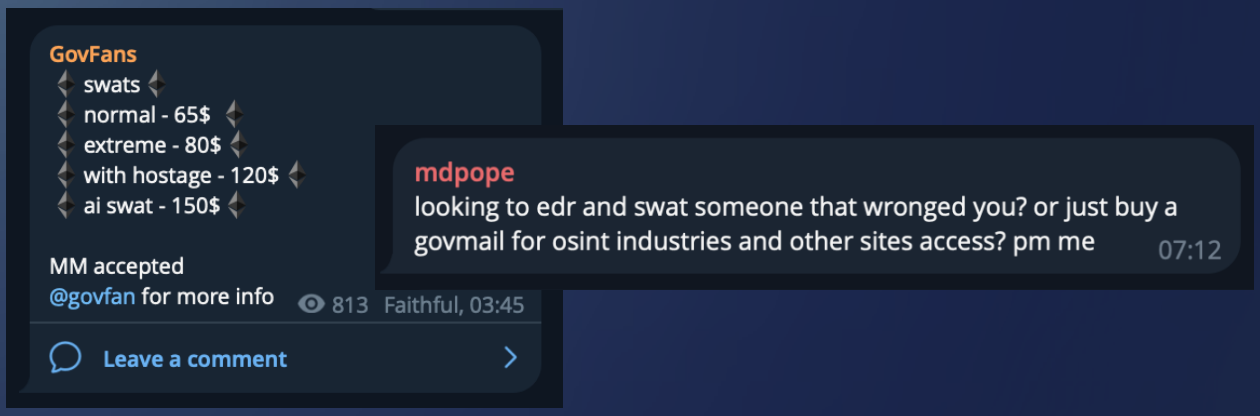
Once obtained, this information gets weaponized across multiple attack vectors. The personal details are posted on dedicated doxxing websites, shared across social media platforms, and distributed through messaging apps to maximize the victim’s exposure and vulnerability.

What This Means

Every EDR could be a weaponized privacy violation waiting to happen. The “emergency” creating pressure to bypass verification might be the very thing putting someone in danger.

The Swatting Connection: The endgame is often “contactless murder”—a particularly dangerous tactic where attackers use the victim’s address to call local police departments with false reports of violent crimes in progress, such as hostage situations or active shooters. The goal is to dispatch heavily armed SWAT teams to the victim’s home, creating volatile situations that can result in injuries and even deaths. Law enforcement agencies report that swatting incidents have increased dramatically as personal address information becomes more readily available through these data request schemes.





2. Supply Chain Attacks Target Your Vendors

On the Rise: Rather than breaking into your systems, criminals are finding increasingly creative vectors into companies.

This shift represents a fundamental change in attack methodology. Traditional cybersecurity focuses on protecting networks, servers, and applications from technical intrusion. But threat actors have realized that the weakest link isn't always technical—it's human, and it's often not even within your direct control.

Business Process Outsourcing (BPO) has become standard practice for customer support operations, allowing companies to scale efficiently while reducing costs. However, these third-party support teams often have the same level of access to sensitive user data as internal employees, but without the same security oversight, monitoring, or loyalty incentives.

The Coinbase Case: The attack against Coinbase exemplifies this new threat vector. Criminals didn't attempt to hack Coinbase's security systems or steal credentials through phishing campaigns. Instead, they identified outsourced customer support agents and successfully bribed them to access and export sensitive user information—including customer names, email addresses, government-issued identification documents, and detailed account information. This data was then leveraged in sophisticated social engineering campaigns designed to trick users into voluntarily transferring their cryptocurrency holdings to attacker-controlled wallets.

What This Means

Your security is only as strong as your weakest vendor. Every team with access to user data is now a potential attack vector.

Why This Matters: These attacks are particularly insidious because they bypass virtually all traditional security controls. The access appears completely legitimate in all logging and monitoring systems—it's coming through official support channels, using proper authentication, and following established procedures. The only anomaly is the motivation of the person making the request, which is nearly impossible to detect through technical means alone.

3. Increasingly Sophisticated Impersonation Techniques

On the Rise: Threat actors now invest serious resources in making their impersonations perfect.

The sophistication of modern impersonation attacks has reached levels that would be impressive if they weren't so dangerous. Gone are the days of obvious phishing emails with spelling errors and generic greetings. Today's threat actors conduct extensive research, invest in high-quality forgeries, and create digital personas that can withstand casual scrutiny.

This evolution reflects the professionalization of cybercrime. As the potential returns from successful data requests have increased, criminal organizations have allocated more resources to perfecting their craft. They study law enforcement procedures, analyze successful legitimate requests, and continuously refine their techniques based on what works and what gets detected.

The Vilebin Group Example: Mentioned in last quarter's report, Vilebin continues to demonstrate the current state of the art in law enforcement impersonation. Using publicly available information about a real police officer from the Erie, Pennsylvania Police Department, they created an elaborate false identity that included multiple fake email addresses using variations of legitimate police domains, complete with official-looking signatures containing real department contact information. They researched actual case procedures and legal codes used by the Erie Police Department, ensuring their requests contained appropriate terminology and reference numbers. Most remarkably, they invested time and resources in creating physical police badges that closely mimicked official designs, photographing these fake credentials to send as "verification" when questioned by suspicious recipients.

The group successfully submitted fraudulent data requests to multiple major technology platforms before being detected, demonstrating that even sophisticated organizations can be fooled by sufficiently well-crafted impersonations.

What This Means

Traditional verification methods—checking email domains, looking for official letterhead—are no longer sufficient. Criminals have professionalized their craft.

Comprehensive List of Compromised Law Enforcement Domains Q2 2025

The following domains have been confirmed compromised or are linked to fraudulent activity in Q2 2025:

Persistently Compromised Domains:

- @zambiapolice.org.zm (Zambia) – This domain remains compromised.
- @poliziadistato.it (Italy) – This domain remains compromised.
- @police.go.th (Thailand) – This domain remains compromised, specifically k******_s*[@]police.go.th and a*.w******[@]police.go.th.
- @policiacivil.ap.gov.br (Brazil) – This domain is compromised. Credentials were found in log leaks. The scope of compromise is unclear, but Kodex is treating all users from this domain as high risk.

Newly Identified Compromised Domains (July):

- @dgfip.finances.gouv.fr (France) – This domain is compromised. User credentials were found in log leaks, and an attempted Kodex registration was flagged and blocked during verification.

Recently Compromised Domains (May-June):

- @police.gov.rw (Rwanda) is a confirmed law enforcement email compromise (LEEC) – the compromise was identified through suspicious account details captured during Kodex registration.
- @policiacivil.pe.gov.br (Brazil) confirmed as compromised.
- @policiacivil.sp.gov.br (Brazil) confirmed as compromised.
- @kppolice.gov.pk (Pakistan) confirmed as compromised.

Cont' (Recently Compromised Domains (May-June):)

- @uige.gov.ao (Angola) is compromised – Dark web communications coupled with threat actor behavior patterns indicated unauthorized access.
- @ukgov.us.kg is a fake domain (Kyrgyzstan) – This is a fraudulent domain designed to mimic a legitimate Kyrgyzstani government entity. The domain was created one week prior to signing up for Kodex.
- @moj.gov.vn (Vietnam) is compromised.

Fraudulent Spoofed Domains Detected

The following domains have been identified as fraudulent lookalikes:

- @mercerislandpolice.org (United States) – This is a fraudulent domain used to impersonate a law enforcement officer from Mercer Island. A user with the email j***.k****[@]mercerislandpolice.org signed up for Kodex the same day the domain was created.
- @cliftonpolice.com (United States) – This is a fake domain impersonating the Clifton Police Department in New Jersey. A user with the email j********[@]cliftonpolice.com attempted to register for Kodex. The legitimate domain is @cliftonpolice.org.
- @greatfallspd.net (United States) is a fake domain. Read more below.
- @guernseypolice.uk (United Kingdom) is a fake domain. Read more below.

Case Study

When Attacks Meet Reality

Rio Concert

2.5 Million Lives at Stake

The Threat

Kodex detected malicious activity from the Rio de Janeiro police domain (@pcivil.rj.gov.br) and implemented security restrictions.

The Race

Despite the restrictions, verified user Commander Alesandro Gonçalves Barreto needed emergency data from Discord about a credible threat to a Lady Gaga concert.

The Save

Kodex's platform intelligence isolated the threat while preserving legitimate access. The commander obtained critical data that helped prevent a planned attack at an event with 2.5 million attendees.

"Kodex was essential in this investigation. The platform acted as a secure bridge between law enforcement and Discord, allowing us to obtain emergency data tied to profiles involved in a serious threat."

— Commander Alesandro Gonçalves Barreto

What We Learned

Surgical security measures can stop bad actors without blocking legitimate emergencies. Platform-level threat intelligence provides visibility that individual organizations simply can't achieve alone.

Coinbase

When Your Help Desk Becomes the Threat

The Attack	Criminals bribed Coinbase's outsourced customer support agents to access sensitive user information—bypassing every security control by working through legitimate support channels
The Damage	Names, email addresses, government ID images, and account data were leaked and used in social engineering attacks designed to steal users' cryptocurrency.
What We Learned	The weakest link isn't always technical—it's human. Any vendor with access to user data needs the same security scrutiny as your core systems.

Vilebin Group

The Professionalizing of Fraud

The Operation	This organized group used real police officer Jason Russell's identity to create jrussell[@]police[.]eriepa[.]org and submit fraudulent data requests across multiple companies.
The Sophistication	They created fake police badges, used proper legal terminology, and researched actual department procedures to make their requests indistinguishable from legitimate ones.
What We Learned	Individual verification tactics are failing. Organizations need systematic approaches that can detect coordinated campaigns across multiple platforms.

Attack Techniques: The Criminal Playbook

The Perfect Impersonation Formula

The modern playbook for law enforcement impersonation has evolved into a systematic process that combines traditional social engineering with sophisticated technical preparation and psychological manipulation.

Step 1: Identity Theft

Threat actors begin by systematically harvesting information from law enforcement agency websites, which typically publish officer names, photographs, contact information, and organizational structures as part of their public transparency efforts. This open-source intelligence gathering extends to social media profiles, news articles featuring officers, and even court documents that mention law enforcement personnel. The goal is to build comprehensive profiles that include not just names and titles, but details about specific cases, departmental procedures, and personal backgrounds that can add authenticity to impersonation attempts.

Step 2: Domain Creation

The technical sophistication of domain registration has increased dramatically. Rather than obvious misspellings, threat actors now register domains that exploit subtle variations in legitimate police domains. For example, using .net instead of .org extensions, or incorporating city names differently (@greatfallspd.net instead of the legitimate @greatfallsmt.net). These domains are often registered through privacy services and paid for with cryptocurrency to avoid detection. The criminals then configure proper email infrastructure, including SPF records and professional signatures, to make their communications appear as legitimate as possible.

Step 3: Documentation Forgery

Perhaps the most concerning development is the investment criminals are making in physical and digital forgeries. These aren't quick photoshop jobs, but thoughtful, time-intensive forgeries. For example, threat actors have made fake police badges by printing them in color on thick, watermarked stock paper, folding them to look uncut, and then placing them in laminated badge holders to mimic authentic credentials. Threat actors also create letterhead templates, case file formats, and legal document structures that match the authentic materials used by the departments they're impersonating.

Step 4: Psychological Manipulation

The social engineering component has become increasingly sophisticated, with criminals developing detailed scripts and training materials that exploit specific psychological triggers. The consistent use of child safety emergencies isn't accidental—it's a calculated exploitation of recipients' moral obligations and legal fears. Phrases like "individual would suffer greatly or die" are specifically chosen to create time pressure that overwhelms careful verification procedures. The practice of CC'ing fake supervisors exploits institutional trust and authority bias, making recipients feel that questioning the request would be inappropriate or insubordinate.

Red Flags to Watch For	
	• Urgent CSAM-related requests with pressure to bypass verification • Slight domain variations (.net vs .org, .uk vs .gov.uk)

The Email Vulnerability Gap

Email remains the primary channel for law enforcement data requests, introducing a critical and persistent security risk that bad actors have systematically learned to exploit. While many organizations have adopted secure portals for routine operations, urgent or emergency law enforcement requests often still rely on email. This reliance is driven by perceived urgency and assumptions that law enforcement lacks access to specialized platforms.

The Problem:

A review of roughly 700 unique companies listed on search.org's ISP list reveals that about **80% accept law enforcement requests via email**—often without the sender verification controls that secure portals provide.

SMTP was never designed for cryptographic sender authentication, making it easy to spoof the "From:" address. While protections like **SPF, DKIM, and DMARC** can help, they are not foolproof:

- **Misconfigurations are common.**
- **Forwarding can break SPF.**
- **A threat actor with stolen credentials (and no MFA) can bypass these protections,** leveraging legitimate DKIM signatures and SPF records to appear completely authentic.

In some cases, forged emails can be detected by analyzing full header chains—such as mismatches between envelope and header "From" addresses or anomalies in "Received" lines. However, this requires manual forensic expertise and still fails to detect account takeovers.

What's Missing:

- **Robust Compromise Detection:** Email headers can reveal spoofing through Received-chain anomalies or mismatched envelope vs. header From, but few orgs actually inspect them—and even header-forensics won't spot a straight account takeover.
- **Account-Takeover Protections:** If an attacker has valid credentials (a LEEC scenario) and there's no MFA, they inherit all existing SPF, DKIM, and DMARC trust—so the usual checks offer zero protection.

- Multi-factor authentication: Email workflows assume "possession of the mailbox = authorization." Unlike secure portals that can require additional verification steps, email-based workflows typically rely solely on the assumption that possession of an email account equals proper authorization.
- Revocation & Audit Control: Once you send data by email, you can't revoke it, limit forwarding, or track downstream copies—leaving sensitive law-enforcement data ungoverned.
- Universal Encryption Adoption: Though S/MIME and PGP exist, most law-enforcement exchanges still fly in plaintext, exposing messages to interception on any hop.

The Solution:

Organizations must transition high-stakes data exchanges to a dedicated, secure verification portal that:

- Validates Session Integrity: Confirm each session is genuine before any data is released.
- Applies Dynamic Risk Controls: Increase scrutiny for higher-risk requests based on real-time signals.
- Protects Data End-to-End: Keep information secured throughout its lifecycle, with no simple "forward" or copy.
- Enables Instant Revocation: Cut off access immediately if anything looks suspicious.
- Maintains Tamper-Proof Records: Store every interaction in a way that can't be altered, so you always know what happened.

Replacing insecure SMTP workflows with a purpose-built, verification-first platform eliminates both spoofing gaps and account takeover risks. This kind of control is something only a true verification portal can deliver.

As evidence of this shift, Europol's SIRIUS Platform published a 2023 survey (p.23) of law enforcement agencies. The findings showed that **66% of respondents preferred submitting requests via an online portal**—a clear signal that the ecosystem is ready for change.

Dark Web Marketplaces: Crime Gets Organized

The commercialization of law enforcement credential theft has reached a level of sophistication that rivals legitimate software-as-a-service businesses. What began as individual hackers selling stolen credentials has evolved into organized marketplaces with customer support, service guarantees, and professional marketing materials.

The Business Model:

Law enforcement email access is now sold like any other commodity, complete with professional marketplaces and customer reviews. These marketplaces operate with the same attention to customer experience as legitimate e-commerce platforms, featuring user ratings, dispute resolution systems, and even technical support for buyers who need help executing their attacks.

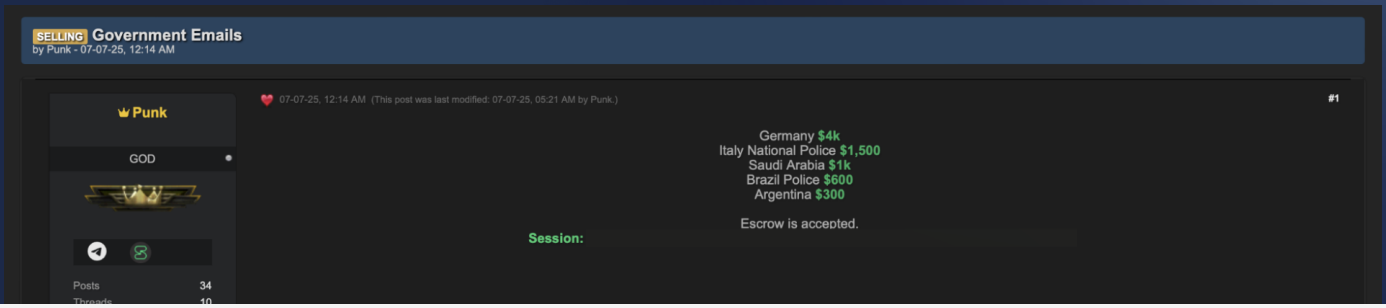
The pricing structure reflects both the value and the risk associated with different types of access. Basic compromised credentials from smaller jurisdictions command lower prices, while access to major metropolitan police departments or federal agencies can cost significantly more. The pricing also varies based on the level of access provided—some sellers offer basic email access, while premium packages include administrative privileges or access to internal law enforcement databases.

The Solution	Price Range	Countries Available
Government email access	$70-100 per account	25+ countries
Complete EDR packages	$200-500	Templates + credentials
Guided attack services	$1,000+	Full-service fraud

What's Being Sold:

The product offerings have expanded far beyond simple credential theft to encompass entire attack ecosystems:

- Access credentials to real law enforcement emails, often sold with guarantees about the duration of access and the authority level of the compromised account
- Template libraries containing pre-written emergency data request formats customized for different types of investigations and various social media platforms, including proper legal language and formatting that mimics authentic requests
- Training courses on social engineering techniques, including video tutorials on voice modulation for phone verification calls and guides to researching target organizations to make requests more convincing
- Consulting services for complex attacks where experienced criminals will personally guide buyers through multi-stage operations, including initial reconnaissance, request submission, and follow-up actions if the first attempt failstestimonials from satisfied customers. This evidence serves both as marketing material for new buyers and as training resources that help improve the overall success rate of these attacks.

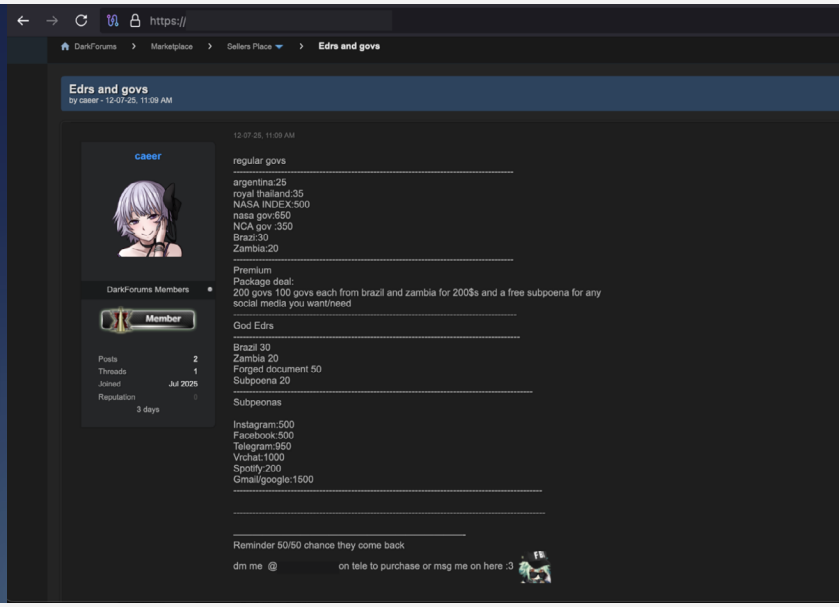


Success Metrics:

The marketplaces maintain extensive documentation of successful operations, including screenshots of actual corporate responses to fraudulent requests and testimonials from satisfied customers. This evidence serves both as marketing material for new buyers and as training resources that help improve the overall success rate of these attacks.

Market Reality Check

When criminals can buy law enforcement email access for less than a nice dinner, traditional verification based on email domains alone becomes meaningless.



The global scope of these operations is particularly concerning. Vendors advertise access to law enforcement credentials from countries across every continent, indicating that this isn't a localized problem but a worldwide criminal enterprise that exploits jurisdictional gaps and varying levels of cybersecurity awareness among different law enforcement agencies.

Defense Blueprint: Your Action Plan

For Companies

Immediate Actions:

- Implement 2-hour “cooling off” periods for all emergency requests
- Require callback verification using only publicly listed agency phone numbers
- Check domain registration dates (recent registrations are highly suspicious)
- Audit all vendors with access to user data, especially BPO providers

Advanced Measures:

- Deploy third-party verification services immune to social engineering
- Create multi-person approval requirements for high-stakes requests
- Share threat intelligence with industry partners
- Document all verification steps for pattern analysis

For Law Enforcement Agencies

Access & Authentication:

- Require 16+ character passwords with phishing-resistant MFA
- Implement time-based access for elevated privileges
- Monitor dark web forums for credential leaks of your domain

Infrastructure Security:

- Update mail servers (especially vulnerable Zimbra installations)
- Implement DMARC, DKIM, and SPF email authentication
- Segment networks to prevent lateral movement after compromise
- Establish incident response procedures with FBI field office contacts

About Kodex

Your Shield Against Sophisticated Threats

Kodex revolutionizes how organizations handle sensitive subpoenas and data requests from law enforcement and government agencies. Founded by a former FBI agent and backed by Andreessen Horowitz, Kodex has become the industry standard for secure data exchange, serving over 90,000 government agents globally and trusted by industry leaders including Coinbase, AT&T, and LinkedIn. Our purpose-built platform transforms a traditionally complex process into a streamlined workflow, helping organizations maintain compliance, strengthen security, and reduce operational costs by millions annually. By bridging the gap between companies and authorized requestors, Kodex ensures that sensitive data is handled with uncompromising security and efficiency.

Kodex's global intelligence network and rigorous law enforcement verification system allows us to detect emerging threats before they appear in traditional security channels. Our threat hunting team uses a six-step intelligence process to identify key threats impacting teams responding to lawful data requests, providing actionable insights to protect your organization.

Take Action Now

The threat actors aren't waiting—and neither should you.

Schedule a Threat Intel Briefing Get personalized intelligence on threats targeting your company
Learn More About Kodex See how we're protecting organizations like yours

Website: https://www.kodexglobal.com/ | Demo: https://www.kodexglobal.com/contact

The criminals have organized. It's time for the good guys to do the same.