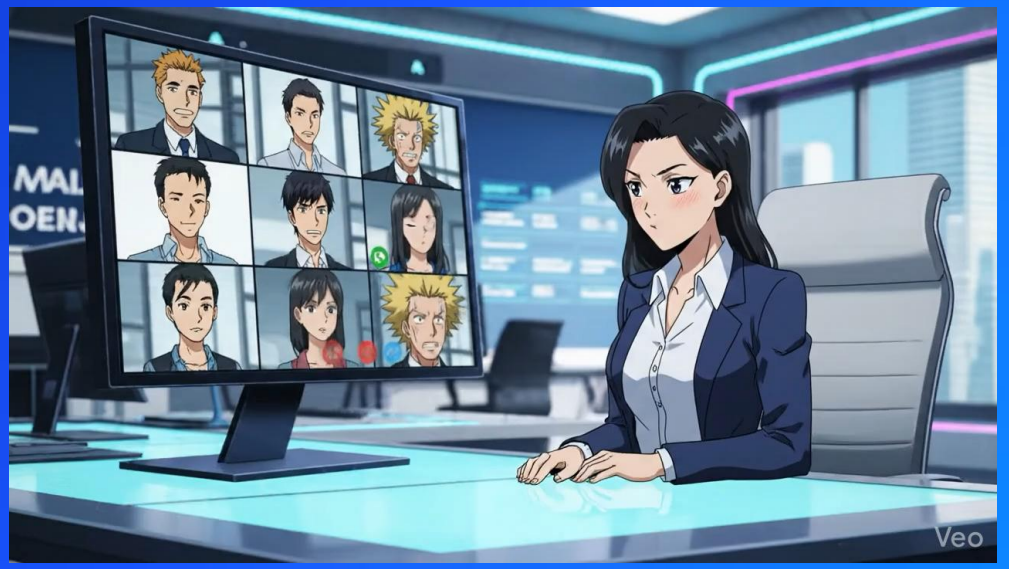
How to Detect Malicious Remote Workers

Could a nation-state threat actor get hired
and stay invisible to your SOC?

JAMES MCQUIGGAN

DPRK Solution – Did you Hire a North Korean?



Did We Just Hire a North Korean?

THE WALL STREET JOURNAL.

North Korea Infiltrates U.S. Remote Jobs—With the Help of Everyday Americans

A LinkedIn message drew a former waitress in Minnesota into a type of intricate scam involving illegal paychecks and stolen data

583 | Gift unlocked article | Listen (13 min)

How comfortable are you to spot deepfakes?

Yes

No

Not Sure

CISSP Certified Information Systems Security Professional
ISC2 Certification

OSC OPEN-SOURCE CERTIFIED

James R. McQuiggan

CISSP | OSC

Advisory CISO & Thought Leader
AI | AI GRC | Agentic AI | Generative AI
Human Risk Management | Risk Management | Cybersecurity

apparentsecurity

Today’s Journey

Overview

Use Cases

SOC Playbook

Attacker's Playbook

Legal Impact

Human Risk

Overview

North Korean
Program Leaders

Foreign-Based
North Korean Employees

US-Based
Criminal Infrastructure

US Company
Remote Employees

Team Managers
&
Tech Employees

Laptop Farms
Fake IDs, etc.

North Korean
Fake Employees

Sending: money, data,
access

High Level Overview

DRPK Education

IT Degree Programs

Premier universities offer strong IT degree programs.

STEM Programs

Universities established hundreds of STEM programs.

Competitive Admission

Only top students are accepted into elite programs.

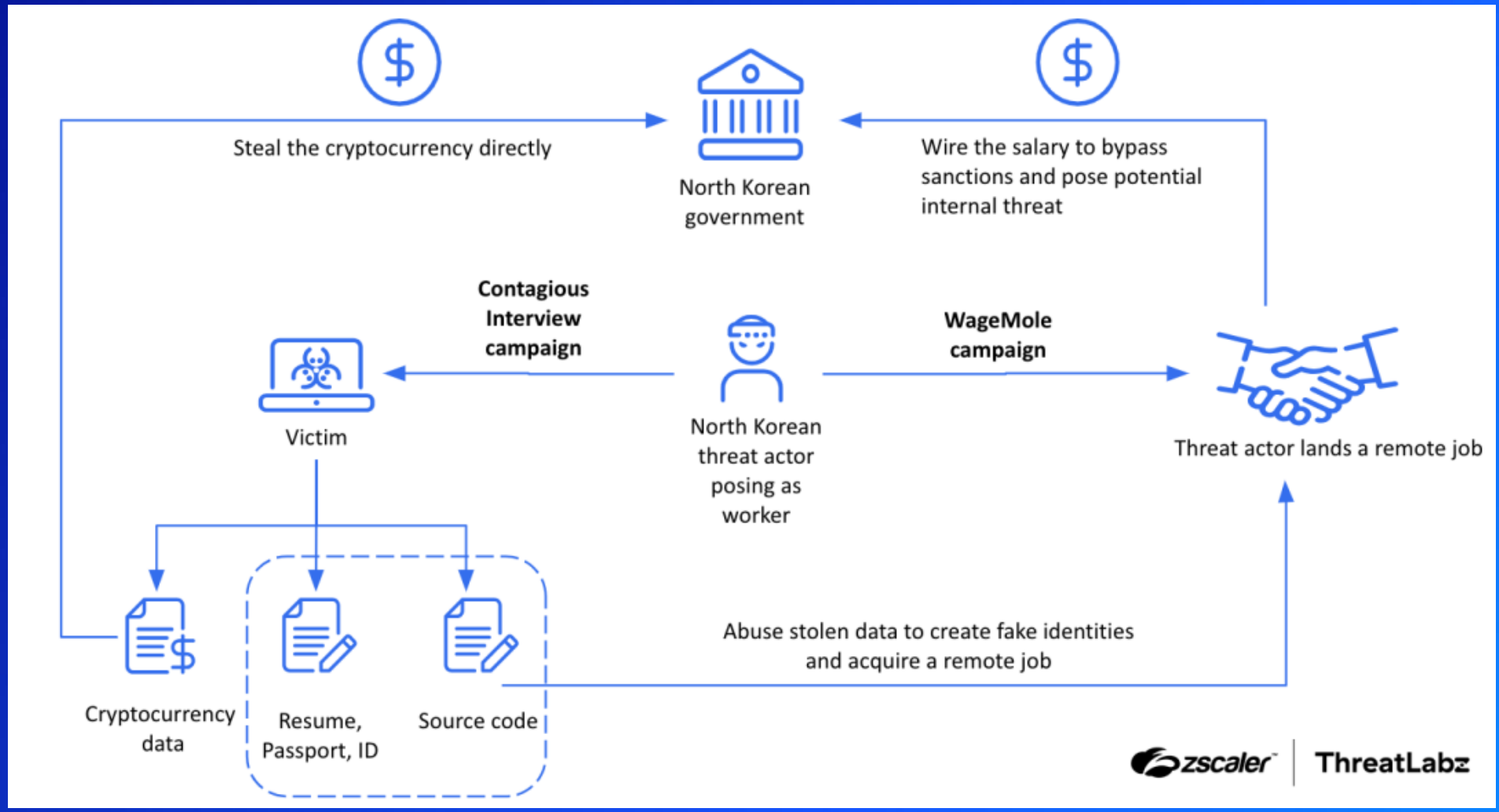
Overseas Training

DPRK IT workers receive additional training overseas.

The Ultimate Inside Threat – DPRK Job Opps

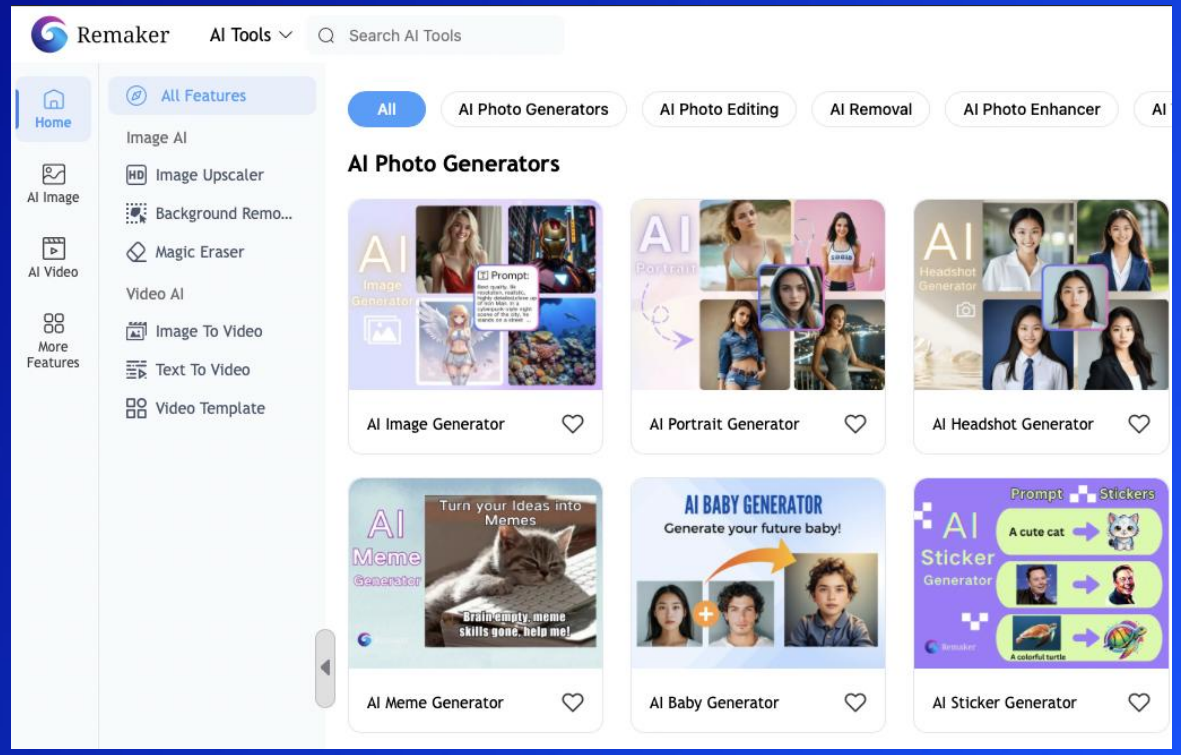
Attacker’s Playbook

Contagious Interview / WageMole Campaigns



Investigations – Crowdstrike / Okta / Unit 42

How Identities Are Built – AI Images

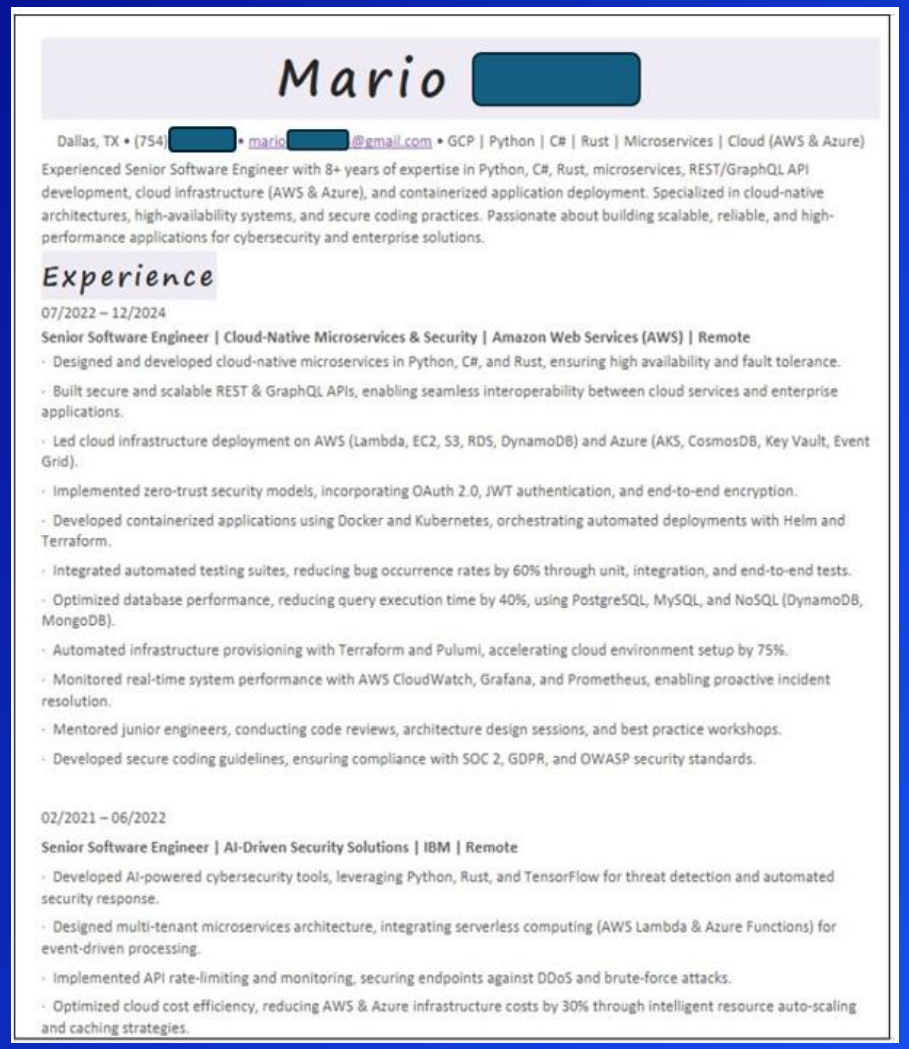


Stock photo

AI Generated

- Stolen SSN's addresses, creds
- Leverage AI generated images

GenAI Resumes



Mario [redacted]

Dallas, TX • (754) [redacted] • mario [redacted] @gmail.com • GCP | Python | C# | Rust | Microservices | Cloud (AWS & Azure)

Experienced Senior Software Engineer with 8+ years of expertise in Python, C#, Rust, microservices, REST/GraphQL API development, cloud infrastructure (AWS & Azure), and containerized application deployment. Specialized in cloud-native architectures, high-availability systems, and secure coding practices. Passionate about building scalable, reliable, and high-performance applications for cybersecurity and enterprise solutions.

Experience

07/2022 – 12/2024

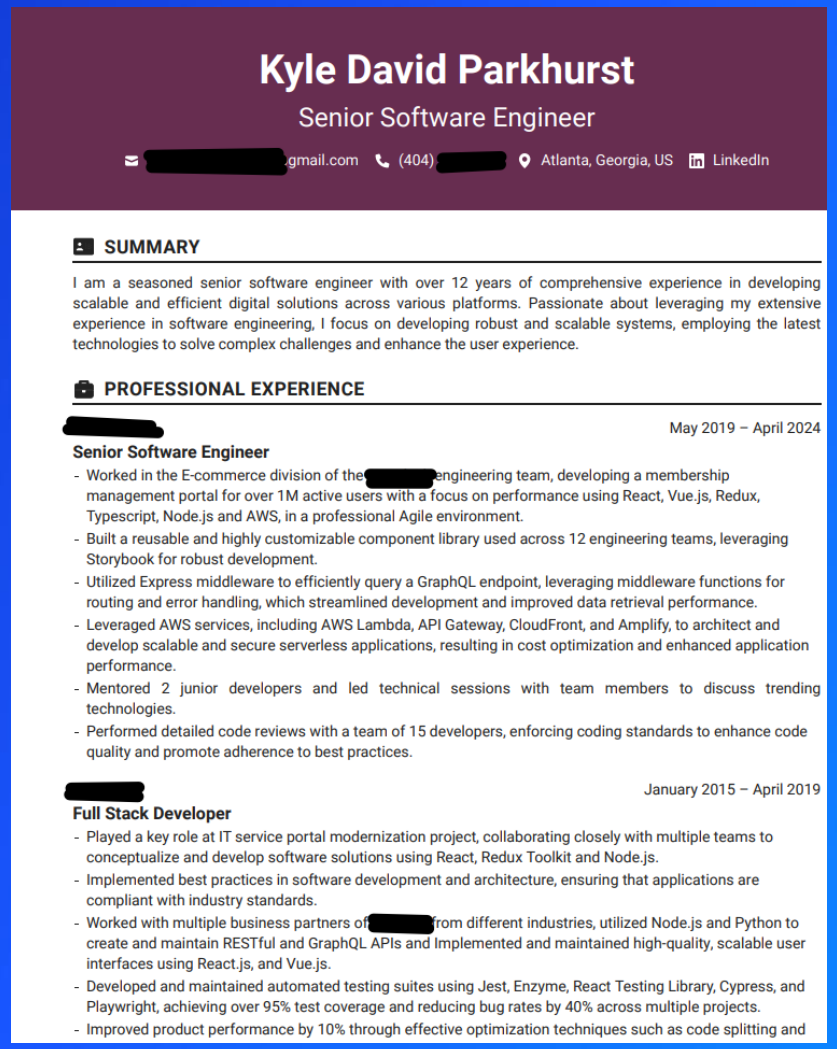
Senior Software Engineer | Cloud-Native Microservices & Security | Amazon Web Services (AWS) | Remote

- Designed and developed cloud-native microservices in Python, C#, and Rust, ensuring high availability and fault tolerance.
- Built secure and scalable REST & GraphQL APIs, enabling seamless interoperability between cloud services and enterprise applications.
- Led cloud infrastructure deployment on AWS (Lambda, EC2, S3, RDS, DynamoDB) and Azure (AKS, CosmosDB, Key Vault, Event Grid).
- Implemented zero-trust security models, incorporating OAuth 2.0, JWT authentication, and end-to-end encryption.
- Developed containerized applications using Docker and Kubernetes, orchestrating automated deployments with Helm and Terraform.
- Integrated automated testing suites, reducing bug occurrence rates by 60% through unit, integration, and end-to-end tests.
- Optimized database performance, reducing query execution time by 40%, using PostgreSQL, MySQL, and NoSQL (DynamoDB, MongoDB).
- Automated infrastructure provisioning with Terraform and Pulumi, accelerating cloud environment setup by 75%.
- Monitored real-time system performance with AWS CloudWatch, Grafana, and Prometheus, enabling proactive incident resolution.
- Mentored junior engineers, conducting code reviews, architecture design sessions, and best practice workshops.
- Developed secure coding guidelines, ensuring compliance with SOC 2, GDPR, and OWASP security standards.

02/2021 – 06/2022

Senior Software Engineer | AI-Driven Security Solutions | IBM | Remote

- Developed AI-powered cybersecurity tools, leveraging Python, Rust, and TensorFlow for threat detection and automated security response.
- Designed multi-tenant microservices architecture, integrating serverless computing (AWS Lambda & Azure Functions) for event-driven processing.
- Implemented API rate-limiting and monitoring, securing endpoints against DDoS and brute-force attacks.
- Optimized cloud cost efficiency, reducing AWS & Azure infrastructure costs by 30% through intelligent resource auto-scaling and caching strategies.



Kyle David Parkhurst

Senior Software Engineer

[redacted] gmail.com (404) [redacted] Atlanta, Georgia, US LinkedIn

SUMMARY

I am a seasoned senior software engineer with over 12 years of comprehensive experience in developing scalable and efficient digital solutions across various platforms. Passionate about leveraging my extensive experience in software engineering, I focus on developing robust and scalable systems, employing the latest technologies to solve complex challenges and enhance the user experience.

PROFESSIONAL EXPERIENCE

[redacted] May 2019 – April 2024

Senior Software Engineer

- Worked in the E-commerce division of the [redacted] engineering team, developing a membership management portal for over 1M active users with a focus on performance using React, Vue.js, Redux, Typescript, Node.js and AWS, in a professional Agile environment.
- Built a reusable and highly customizable component library used across 12 engineering teams, leveraging Storybook for robust development.
- Utilized Express middleware to efficiently query a GraphQL endpoint, leveraging middleware functions for routing and error handling, which streamlined development and improved data retrieval performance.
- Leveraged AWS services, including AWS Lambda, API Gateway, CloudFront, and Amplify, to architect and develop scalable and secure serverless applications, resulting in cost optimization and enhanced application performance.
- Mentored 2 junior developers and led technical sessions with team members to discuss trending technologies.
- Performed detailed code reviews with a team of 15 developers, enforcing coding standards to enhance code quality and promote adherence to best practices.

[redacted] January 2015 – April 2019

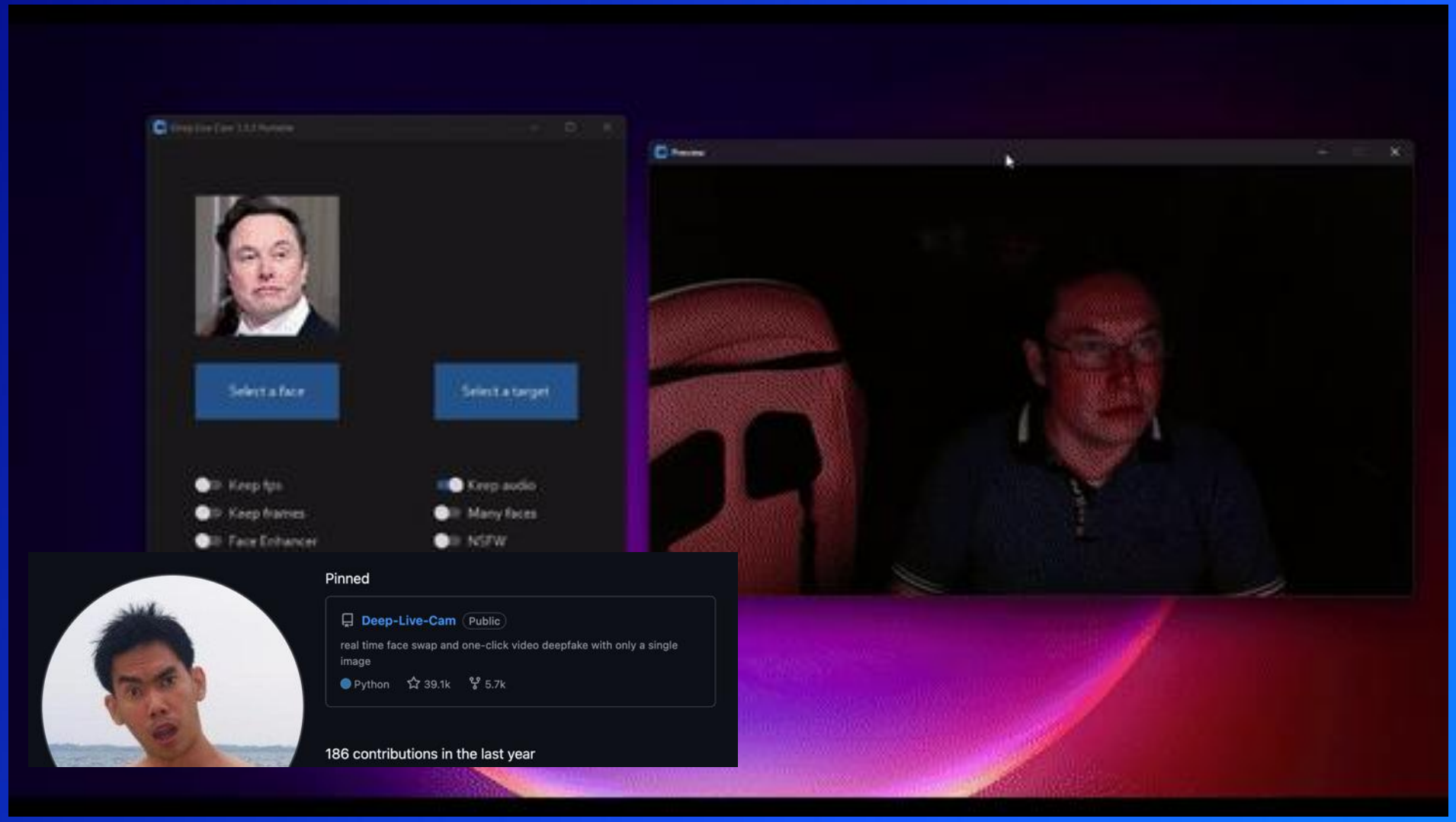
Full Stack Developer

- Played a key role at IT service portal modernization project, collaborating closely with multiple teams to conceptualize and develop software solutions using React, Redux Toolkit and Node.js.
- Implemented best practices in software development and architecture, ensuring that applications are compliant with industry standards.
- Worked with multiple business partners of [redacted] from different industries, utilized Node.js and Python to create and maintain RESTful and GraphQL APIs and Implemented and maintained high-quality, scalable user interfaces using React.js, and Vue.js.
- Developed and maintained automated testing suites using Jest, Enzyme, React Testing Library, Cypress, and Playwright, achieving over 95% test coverage and reducing bug rates by 40% across multiple projects.
- Improved product performance by 10% through effective optimization techniques such as code splitting and

Stateside Assistance

- Physical U.S. address for laptop delivery
- Hosting of company-issued devices
- Forwarding of payroll deposits
- Management of stolen U.S. identities for IRS reporting
- Remote access software installation on company laptops
- Accepting payments transfer to NK
- Help with fake identities
- Provide references

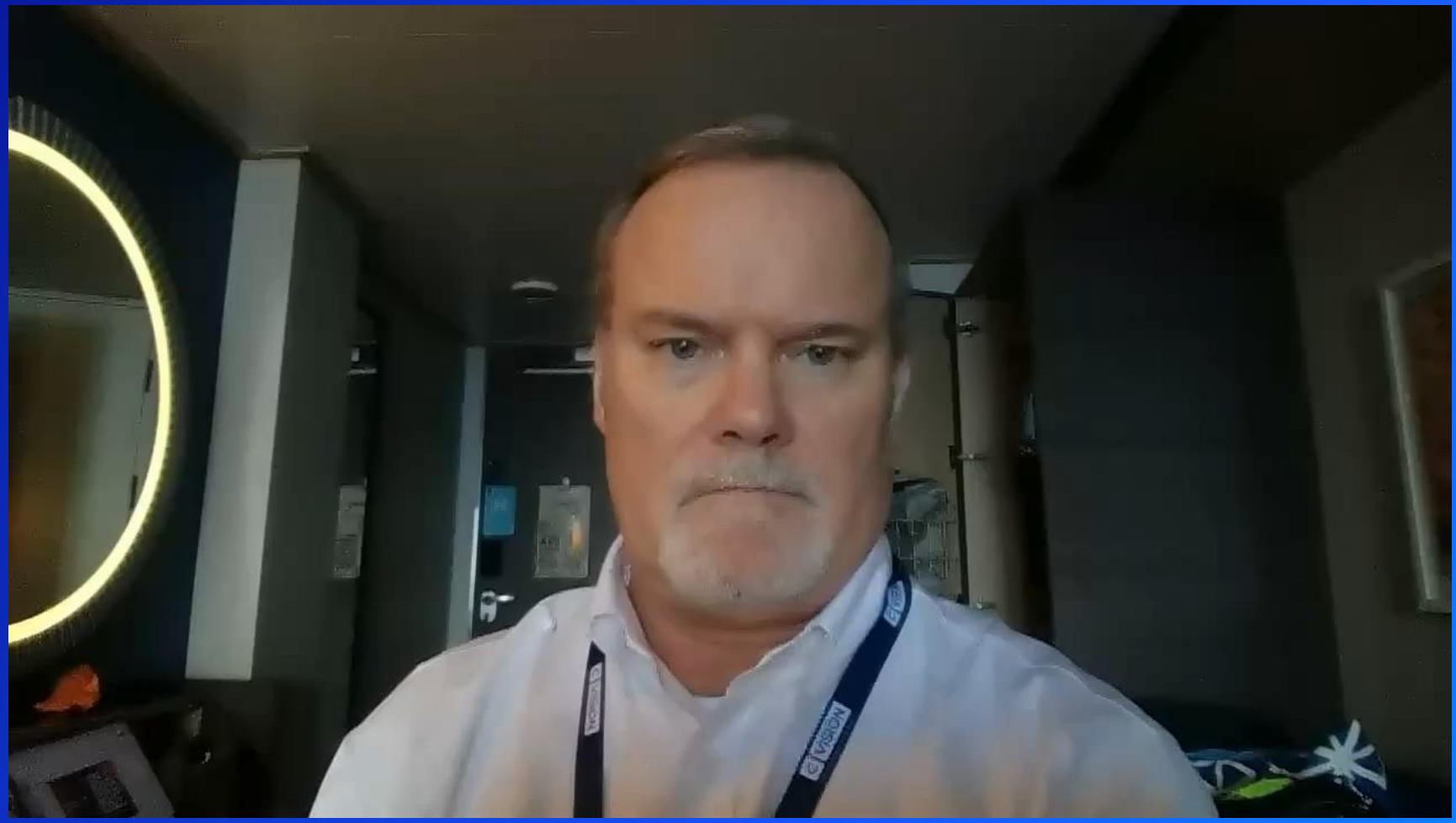
Face Swap / Voice Cloning & Webcams → LIVE Deepfakes



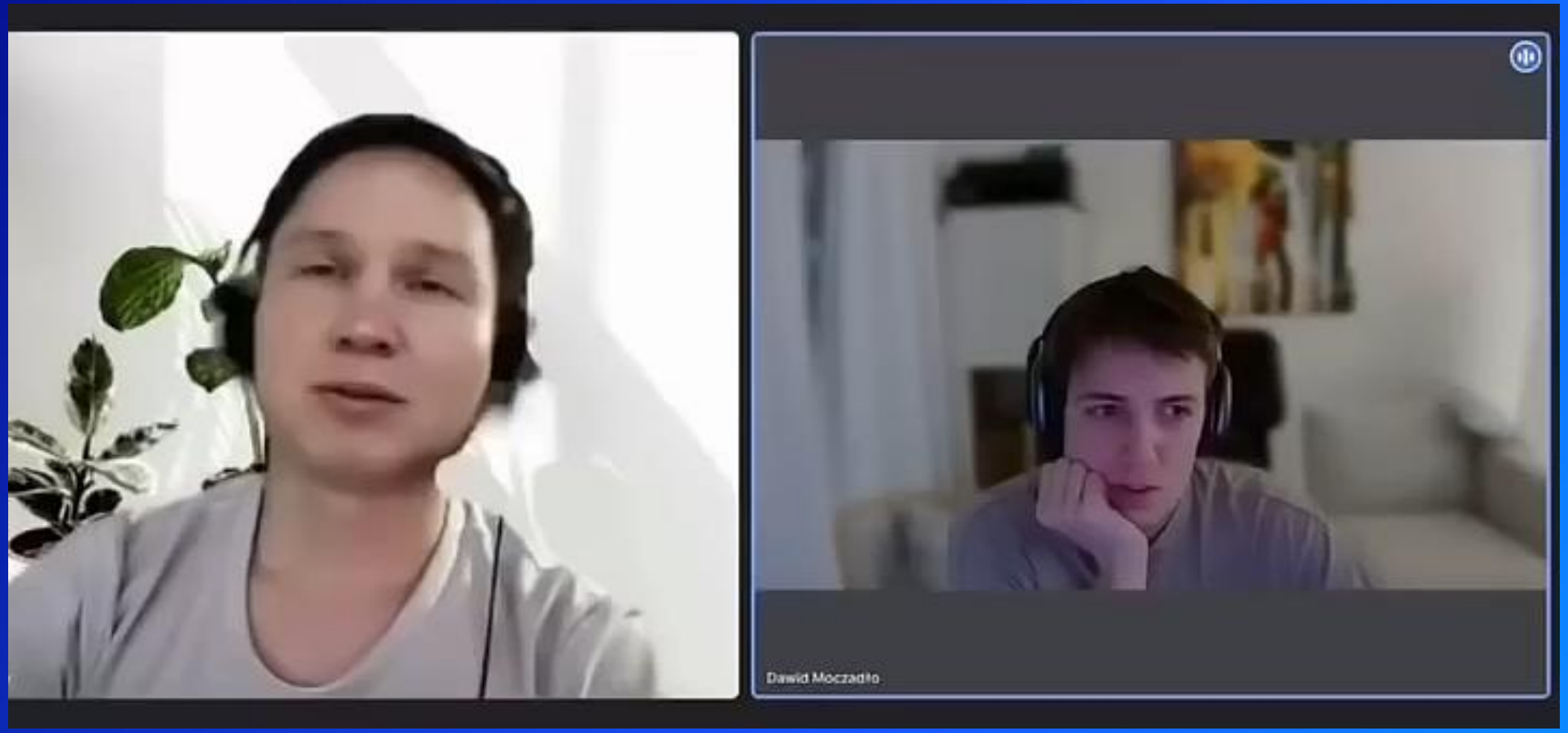
DEMO

FaceSwap & Real Time Voice Content (RVC)

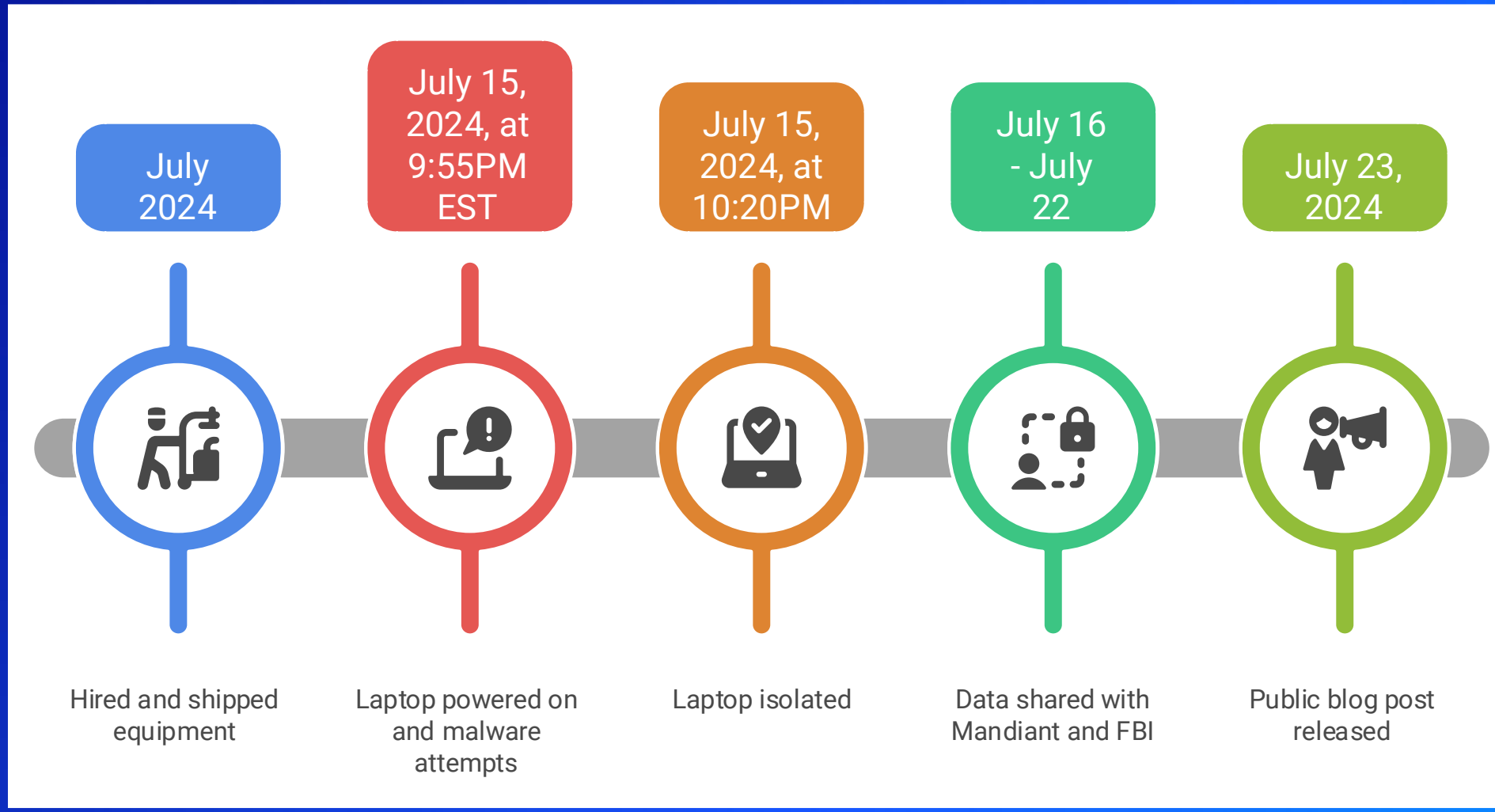
Deepfake Video Swap



Video Camera Real time Video Deepfake Face Swap Interview

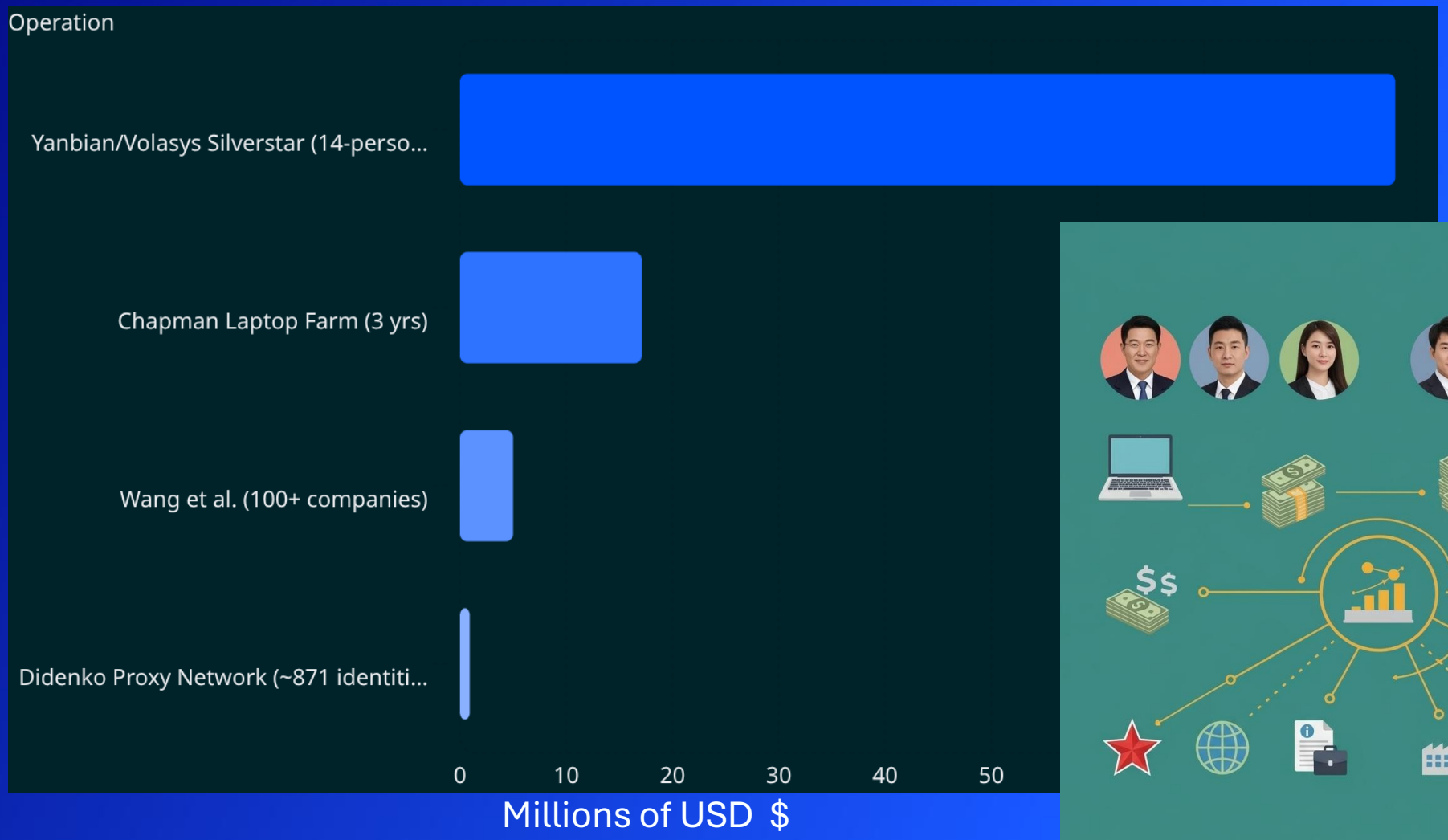


KnowBe4 Use Case – July 2024



Legal Impact

DOJ Operations



NK Farmers Arrested

PRESS RELEASE

Fourteen North Korean Nationals Indicted for Carrying Out Multi-Year Fraudulent Information Technology Worker Scheme and Related Extortions

Thursday, December 12, 2024

For Immediate Release
Office of Public Affairs

Justice Department Continues Efforts to Seize the Illicit Proceeds of the Scheme

Note: View the indictment here and FBI Wanted Posters here.

A federal court in St. Louis, Missouri, yesterday indicted 14 nationals of the Democratic People's Republic of North Korea (DPRK or North Korea) with long-running conspiracies to violate U.S. sanctions and to commit wire fraud, money laundering, and identity theft. Specifically, the conspirators, who worked for DPRK-controlled companies Yanbian Silverstar and Volasys Silverstar, located in the People's Republic of China (PRC) and the Russian Federation (Russia), respectively, conspired to use false, stolen, and borrowed identities of U.S. and other persons to conceal their North Korean identities and foreign locations and obtain employment as remote information technology (IT) workers for U.S. companies and nonprofit organizations.

The conspirators, some of whom were ordered by their superiors to earn at least $10,000 per month, generated at least $88 million throughout the approximately six-year conspiracy. In multiple instances, the conspirators supplemented their employment earnings by stealing sensitive company information, such as proprietary source code, and then threatening to leak such information unless the employer made an extortion payment. Ultimately, the conspirators used the U.S. and PRC financial systems to remit the proceeds of their activity to accounts in the PRC for the ultimate benefit of the DPRK government.

Justice Department Announces Coordinated, Nationwide Actions to Combat North Korean Remote Information Technology Workers' Illicit Revenue Generation Schemes

Monday, June 30, 2025

Share

For Immediate Release
Office of Public Affairs

Law Enforcement Actions Across 16 States Result in Charges, Arrest, Plea Agreement and Seizures of 29 Financial Accounts, 21 Fraudulent Websites, and Approximately 200 Computers

Note: *This press release has been updated to reflect new information regarding the guilty plea of one defendant in the District of Massachusetts.*

https://www.justice.gov/archives/opa/pr/fourteen-north-korean-nationals-indicted-carrying-out-multi-year-fraudulent-information
https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote

New Jersey

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA

v.

(1) ZHENXING WANG,
a/k/a "Danny Wang"
(2) JING BIN HUANG,
a/k/a "靖斌 黄"
(3) BAOYU ZHOU,
a/k/a "周宝玉"
(4) TONG YUZE,
a/k/a "佟雨泽"
(5) YONGZHE XU,
a/k/a "徐勇哲"
a/k/a "يونجزهي أكسو"
(6) ZIYOU YUAN,
a/k/a "زيو"
(7) ZHENBANG ZHOU,
a/k/a "周震邦"
(8) MENGTING LIU, and
a/k/a "劉 孟婷"
(9) ENCHIA LIU,
a/k/a "刘恩嘉"

Defendants.

Criminal No. 25cr10273 NMG-MPK

Violations:

Count One: Conspiracy to Commit Wire and Mail Fraud (18 U.S.C. § 1349)

Count Two: Money Laundering Conspiracy (18 U.S.C. § 1956(h))

Count Three: Conspiracy to Commit Identity Theft (18 U.S.C. §§ 1028(a)(7) and (f))

Count Four: Conspiracy to Damage a Protected Computer (18 U.S.C. § 371)

Count Five: Conspiracy to Violate the International Emergency Economic Powers Act (50 U.S.C. §§ 1705(a) and (c))

Forfeiture Allegations: (18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c); 18 U.S.C. §§ 981(a)(1) and (a)(2)(B), 1028(b)(5), 1030(i); and 19 U.S.C. § 1595a(d))

INDICTMENT

At all times relevant to this Indictment:

WANTED BY THE FBI

FRAUDULENT REMOTE IT WORKERS FROM DPRK

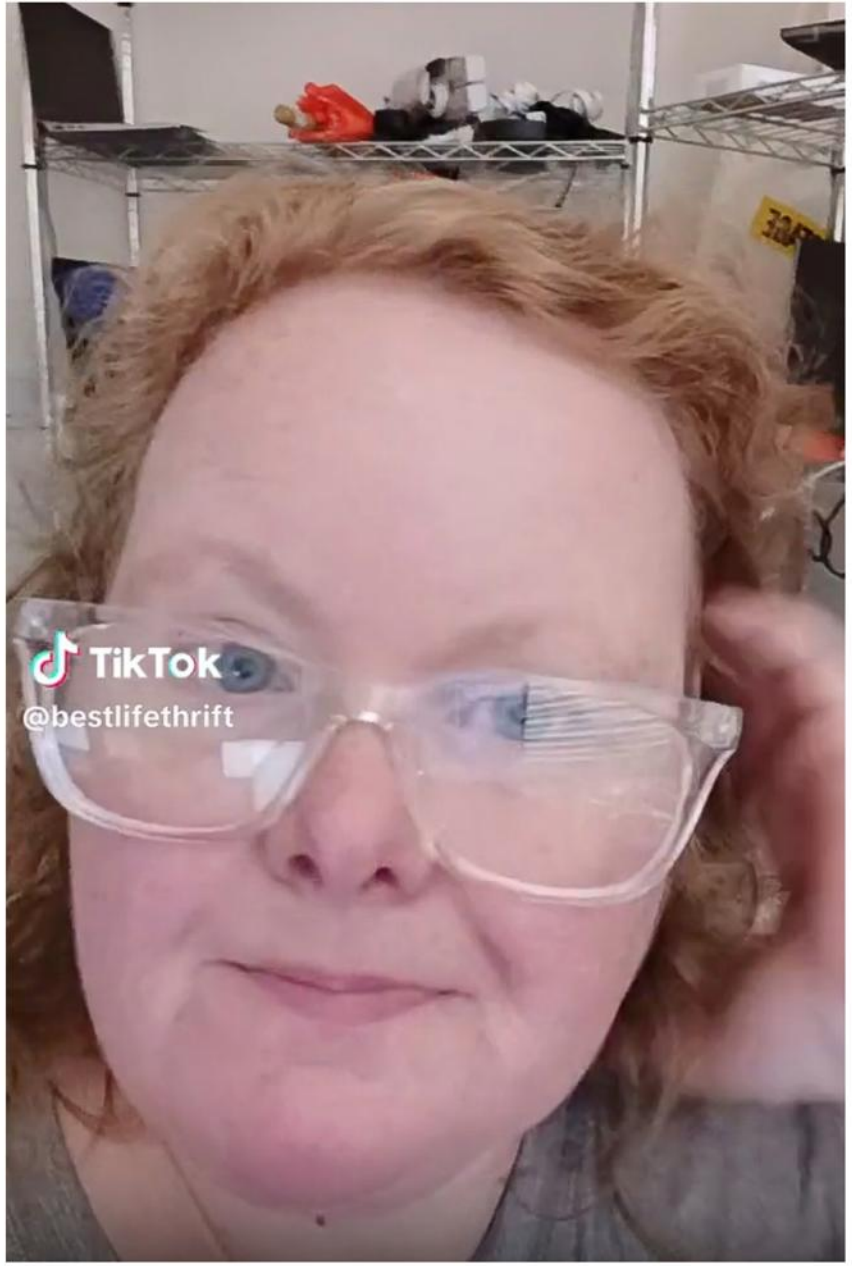
Wire Fraud Conspiracy; Wire Fraud; Money Laundering Conspiracy

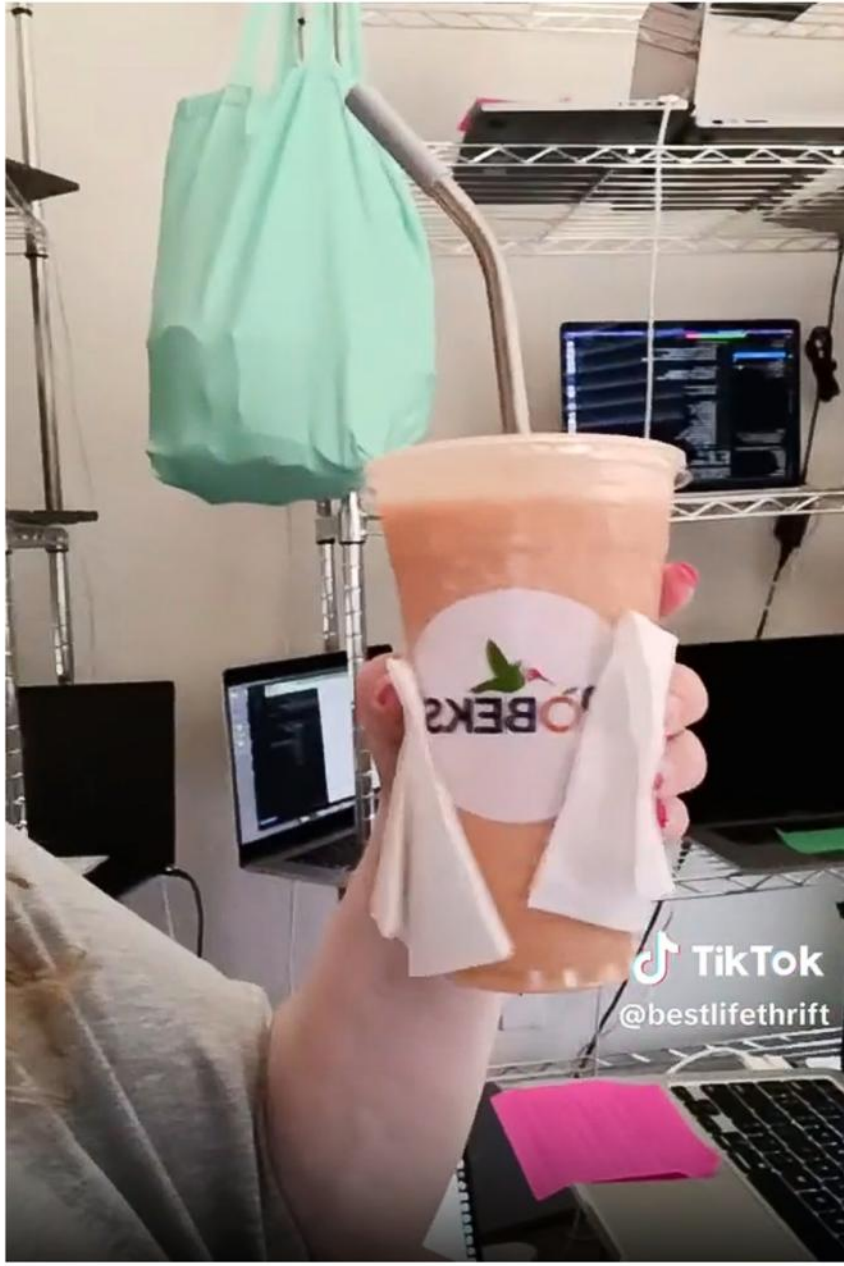

Kim Kwang Jin


Kang Tae Bok


Jong Pong Ju


Chang Nam Il





Screenshots from Chapman's June 2023 Tiktok video with laptops in the background.

Companies Infiltrated — The Numbers

309

Companies
Chapman Operation
Operation

100+

Companies
Wang et al.

200

FBI Victim Notifications

29

Laptop Farms Raided

"There are hundreds of Fortune 500 organizations that have hired these North Korean IT workers. Literally every Fortune 500 company has at least dozens, if not hundreds, of applications."

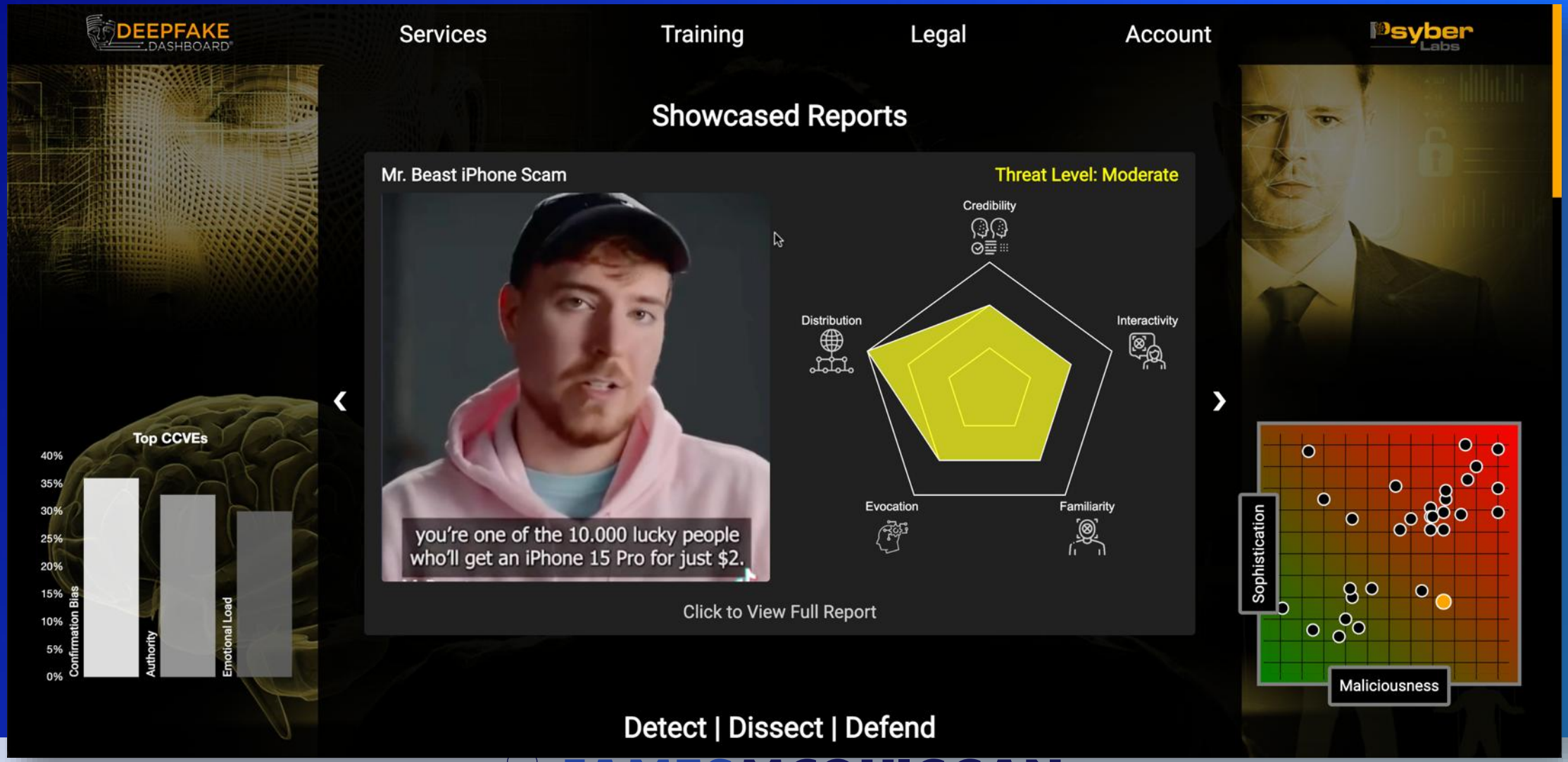
- Mandiant CTO Charles Carmakal, RSAC 2025


JONG SONG HWA
RI KYONG SIK
KIM RYU SONG
RIM UN CHOL
KIM MU RIM
CHO CHUNG POM


SON UN CHOL
CHOE JONG YONG
JANG CHOL MYONG
JONG KYONG CHOL
HYON CHOL SONG
SOK KWANG HYOK

SOC Playbook

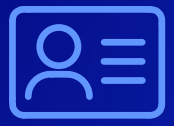
Technology - Deepfake Dashboard



12 Best AI Deepfake Detector Tools

Detecting VOIP Numbers & Identity

SOC Telemetry



Identity Logs

- Concurrent logins from geographically impossible IP pairs;
- VPN origin flags in Okta/Azure AD;
- new RMM tool installation events.
- **Astrill VPN ASN traffic** is a primary indicator.

Endpoint / EDR

- RustDesk, AnyDesk, TinyPilot, VS Code Dev Tunnels
- USB device insertion
- Raspberry Pi connections
- Session / Log file manipulation

Network

- Traffic to Astrill VPN ASNs
- Unique or odd outbound traffic to personal GitHub repos
- Large data transfers during off-hours

DLP

- Unusual volume of code repository downloads
- SharePoint/OneDrive bulk access
- email forwarding rules created by new hires. Red

Hiring Flags

Reused VoIP Numbers or Email Addresses	• Same phone #, email appearing across multiple applicant resumes
Address Mismatch for Laptop Delivery	• Application address differs from resume
Camera Hesitancy	• Reluctance to turn on webcam during interviews or show physical environment
3rd Party Device Forwarding	• Applicant wants laptop forwarded to another address (laptop farm)

HR – Hiring Tips

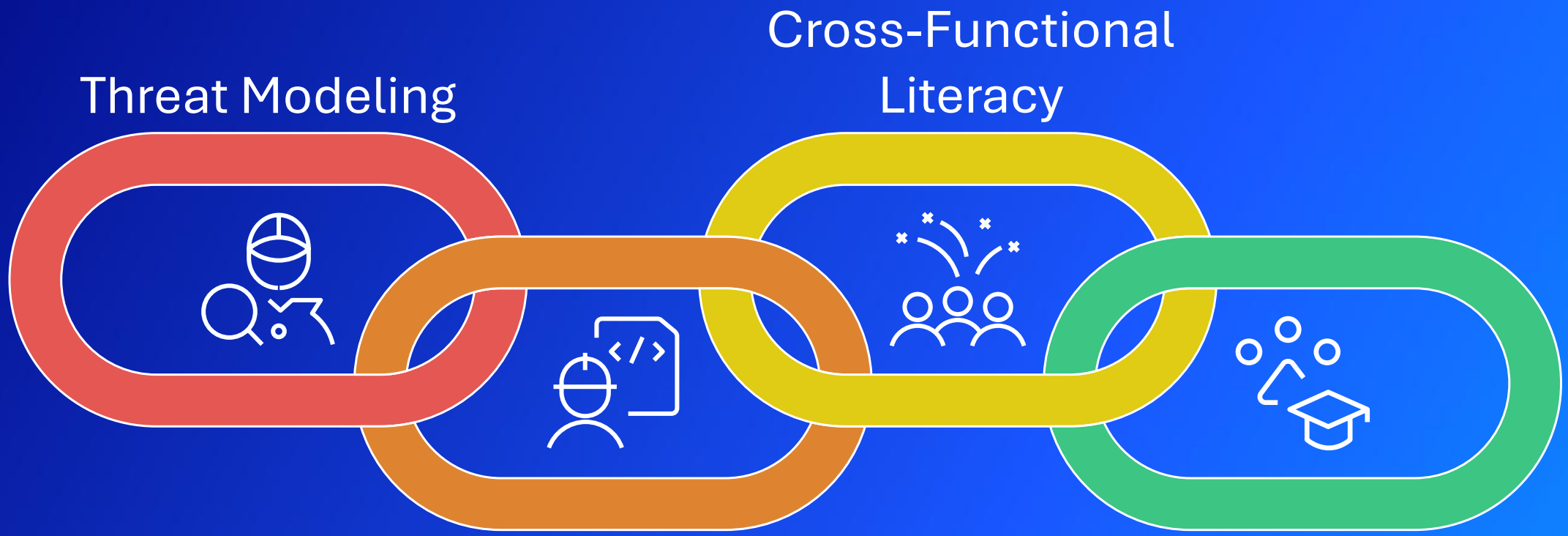
BE CURIOUS

Ask questions about their surroundings


FAKE IDENTITY
SAMPLE DATA ONLY
ACCESS DENIED
SAMPLE IDENTITY
ACCESS DENIED
TEST PROFILE
SAMPLE DATA ONLY

Human Risk

AI First Ready Security Team



People – What Should We Be Asking?

~~Is this a deepfake?~~

Consider these questions...

Apply the FAIK Factor Framework

F **Freeze & Feel**

A **Analyze the Narrative & Emotional Triggers**

I **Investigate (Claims, Sources, etc.)**

K **Know, Confirm, & Keep Vigilant**

Courtesy: Perry Carpenter: FAIK Files

Using Questions/Be Curious

"What is that book that you recommended to me?"

TRUST & VERIFY

BE SKEPTICAL

POLITELY PARANOID

Most Secure Woman?

MFA

Emma Faye

Multifactor Authentication

Questions?

300+ companies in one operation

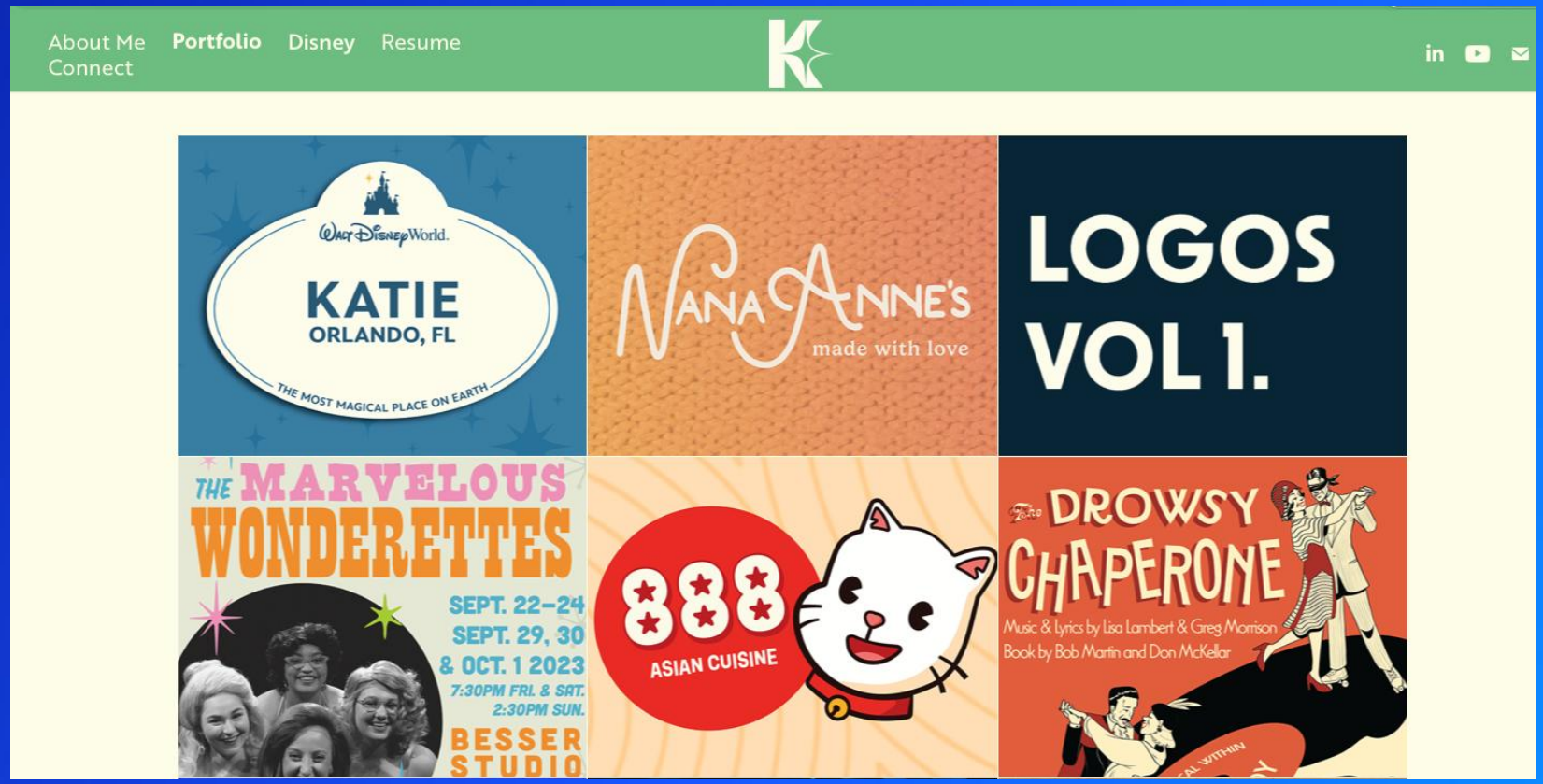
They’re using AI too for images and resumes

Key Takeaways

Threat Hunting

Extortion Can Happen

Graphics Provided by…



katiemcquiggan.com