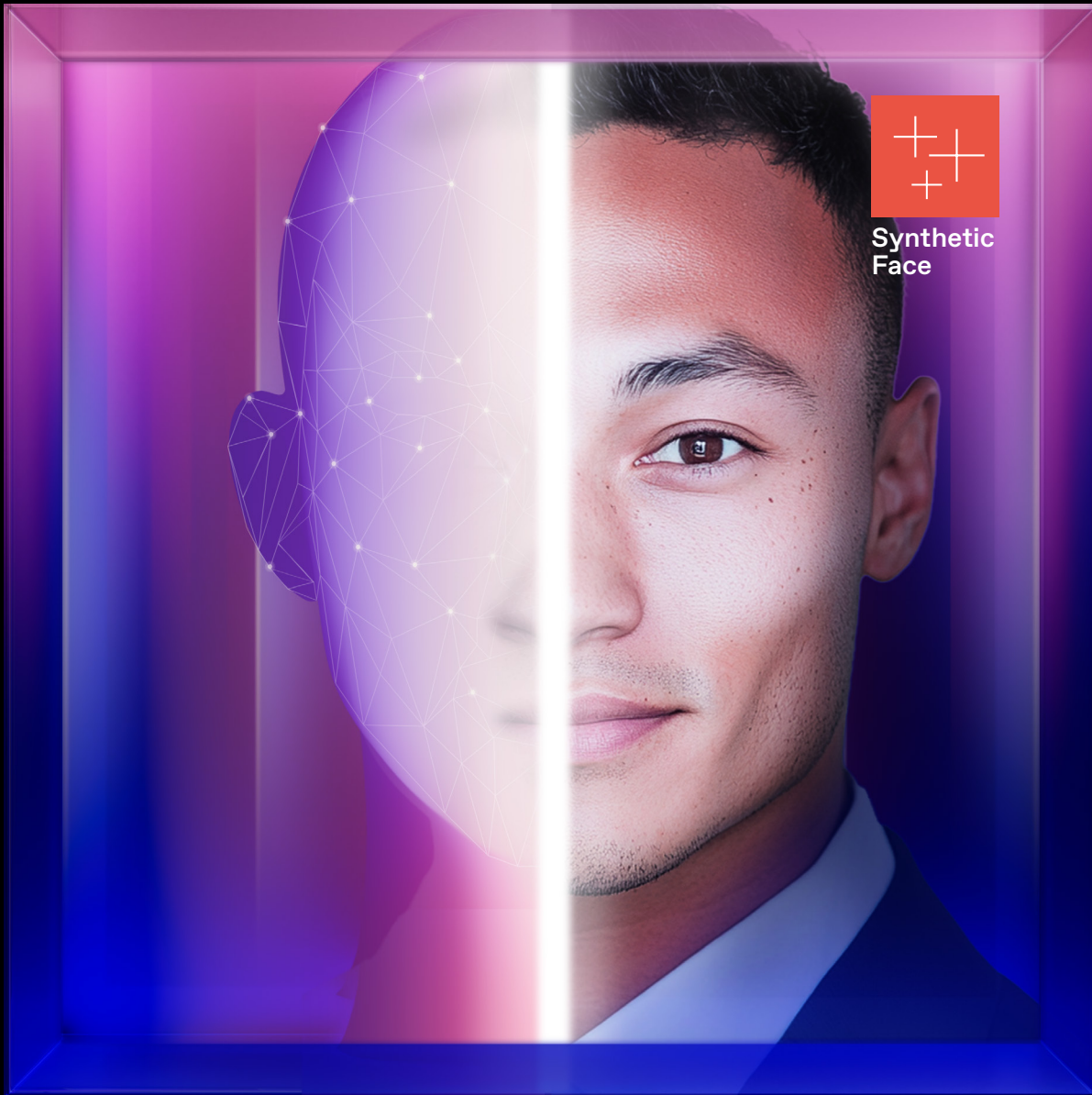


GetReal.



The Hiring Kill Chain: Exposing Synthetic Content, Candidate Fraud, and Imposters in the Talent Pipeline.

A Framework for Disrupting Threat Actors
Before They Become Insider Threats.



From ancient betrayals in the corridors of power to Cold War double agents, insider threats have long been part of history. But for most business leaders, malicious insiders seemed more like a spy movie plotline than a real concern. The threat felt distant, something for the most sophisticated financial-services firms and IP-heavy industries such as pharmaceuticals, manufacturing, and defense.

Today, insider risk has taken on new dimensions. Several Fortune 500 executives have shown me two photos: one of a new hire on their first day and another of the individual who interviewed for the position. Their faces look nothing alike, a clear signal we need to reconsider our assumptions.

Over the past 30 years, nearly every organization and nation-state has come to rely on technology to engage with their audiences and stakeholders. Mission-critical business processes are now digitized—fully or partially—and offer customers, partners, and ecosystems some degree of access. This digital transformation has spawned new vulnerabilities. Adversaries can remotely infiltrate systems and exfiltrate sensitive data and IP in seconds, no physical insiders stealing physical assets necessary.

While countries like China have long engaged in planting operatives to conduct corporate espionage (costing the U.S. economy an estimated \$250 - \$600 billion annually), insider risk has grown beyond the realm of intelligence agencies. While awareness of insider risk increased, it was still underestimated and often treated as a fringe threat.

Things have changed. Generative AI tools forge identities, fabricate resumes, and create convincing deepfakes in minutes. When a person's name, image, voice, or video likeness can be faked at scale, who or what can we trust? Can we still rely on what well-intentioned employees hear and see as the "last control point"? We can't. Research shows the average person can no longer reliably distinguish synthetically generated content from reality.

We've reached the point where trust itself is not just at risk, but under attack—and now we have a real problem. It's already playing out in corporate hiring pipelines.



Generative AI tools forge identities, fabricate resumes, and create convincing deepfakes in minutes. When a person's name, image, voice, or video likeness can be faked at scale, who or what can we trust? Can we still rely on what employees hear and see as the "last control point"? We can't.

What was once the domain of well-funded nation-states is now within reach of individuals and resource-poor but determined actors. Some candidates exaggerate skills and qualifications and have associates complete their work assignments. Others hold multiple full-time positions and outsource their roles to contractors. State-sponsored actors such as North Korean remote IT workers coordinate with a web of conspirators to embed themselves in corporate systems, escalate privileges, stage malware, and more.

We need to rethink the frontlines of organizational risk. GenAI has introduced new attack vectors, particularly in newly digitized human resources and recruiting processes. In the post-COVID era of remote work and digital-first hiring, adversaries now target the proverbial front door, while attention is focused on the back door: infrastructure vulnerabilities.

This paper aims to shed light on the dramatic rise of risk in the recruiting process—and how GenAI has transformed the insider threat from a niche concern to a mass-market attack vector, seemingly overnight.

Matthew Moynahan
Chief Executive Officer
GetReal Security

¹ "Executive Summary - China: The Risk to Corporate America." FBI. Retrieved July 16, 2025 from [here](#)

In the pages that follow, we will:

→ Highlight key hiring process vulnerabilities exploited by threat actors using AI-fueled deception

→ Introduce a “hiring kill chain” framework designed to disrupt imposters before they can infiltrate enterprises

→ Demonstrate why digital content verification and deepfake detection is essential in detecting and stopping imposters earlier in the hiring lifecycle

Will the Real Job Candidate Please Stand Up?

Thousands of North Korean operatives securing remote IT jobs and infiltrating corporate systems at Fortune 500 companies² highlight a growing and underappreciated threat: candidate fraud. Adversaries have shifted focus to HR departments and hiring processes—soft targets largely overlooked by traditional cybersecurity measures.

HR and recruiting, long considered low-risk administrative functions, have become a critical vulnerability in the corporate attack surface. Yet, talent professionals typically lack cybersecurity and identity verification training and tools to detect sophisticated impersonation and fraud.

Candidate fraud extends beyond operatives working for sanctioned nation-states. It includes applicants who exaggerate qualifications, outsource their work, and/or use stand-ins for interviews and assessments. It also includes individuals holding multiple full-time jobs (i.e., “polyworking” or “overemployment”) and delegating tasks to third parties. At the more sophisticated end, it involves state-sponsored actors or criminal networks embedding malicious insiders.

While North Korean operations in this area have received the most media attention lately, similar tactics can be employed by other adversarial nation-states, cybercriminal groups, and financially motivated fraudsters. Motivations vary: from quietly collecting paychecks to send back to headquarters, to stealing intellectual property, establishing backdoors for persistent access, or staging malware for future, broader-scale disruption. In some cases, the hiring organization may be an indirect target in a supply chain attack. For example, a software vendor may hire an imposter whose objective is to steal source code for a particular app deployed by a more valuable downstream target.

What unites these threats is the use of synthetic media and personas. This can include AI-generated or manipulated social media profiles, portfolio websites, resumes, identity documents, and in some cases real-time deepfake audio and video—all designed to bypass human scrutiny and technical controls during the hiring process.

Traditional safeguards such as human intuition, background checks, and identity verification fail to flag these fabrications, as evidenced by hundreds of corporations that have fallen victim. As a result, untrustworthy actors gain unfettered access to corporate systems and opportunities to deceive employees, partners, and customers in pursuit of financial gain, data exfiltration, trade secret theft, espionage, or business disruption.

Recruiters, HR teams, hiring managers, interviewers, and staff-at-large must be educated and empowered with new technology solutions to fight this AI-fueled threat to the hiring lifecycle.

This brief is intended to help executives, cybersecurity leaders, and HR teams understand the critical vulnerabilities in digital-first hiring, the severity and impact of candidate fraud and imposters, shortcomings in current defenses, and the urgent need for a new approach.

² “Guidance on the Democratic People’s Republic of Korea Information Technology Workers.” U.S. Department of the Treasury. May 16, 2022. Retrieved July 16, 2025 from [here](#)

Why this matters: The costs of Job Candidate deception

THE WALL STREET JOURNAL.

North Korean imposter “Laptop farm” siphons \$17.1M in paychecks from 300 companies

“...a series of custom-written programs designed to get around antivirus software and firewalls [gave] the North Koreans a virtually undetectable back door into the corporate network.”

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

Understanding Deception in the Hiring Process

Candidate deception can occur at different stages of the hiring lifecycle and take various forms:

- **Impersonation:** A candidate applies and is hired under a misrepresented, stolen, borrowed, or synthetic ID
- **Proxy or stand-in interviewee:** An accomplice poses as the candidate during interviews or technical assessments
- **Fake references:** Co-conspirators impersonate professional references to vouch for the candidate
- **Overemployment (polyworking):** The candidate conceals simultaneous employment with multiple companies
- **Signing bonus theft:** A candidate accepts a signing bonus but never reports for work

To carry out these types of deception, adversaries increasingly use generative AI to create digital content to corroborate the fake identity. Content may include fake resumes, certifications, employment histories, work-product portfolios, profiles and profile pictures, staffing agencies, identity documents, audio files, video files, and more. Imposters have also started using real-time deepfake audio and/or video to maintain the facade during live interviews and other calls.³

A deceptive job application can quickly escalate into a serious cybersecurity, compliance, or operational threat. Even before they're hired, as an adversary gains increasing access to corporate personnel and systems as part of the hiring process, the risk and potential damages increase.

Regardless of an imposter's origin or motive, hiring one grants a dishonest actor internal access to corporate systems – making candidate fraud and imposter hiring not just an HR issue, but a threat affecting the entire enterprise.

³ “Expert Advice: How to screen and interview candidates who want to use AI tools.” HR Executive. May 28, 2025. Retrieved June 2, 2025, from [here](#).

Why this matters: The costs of Job Candidate deception

POLITICO

Numerous enterprises falling victim and struggling to stop the spread

“I’ve talked to a lot of CISOs at Fortune 500 companies, and nearly every one ... has admitted they’ve hired at least one North Korean IT worker, if not a dozen or a few dozen.”

Tech companies have a big remote worker problem: North Korean operatives

⁴ “Expert Advice: How to screen and interview candidates who want to use AI tools.” HR Executive. May 28, 2025. Retrieved June 2, 2025, from [here](#)

⁵ “AI Impact on Hiring Survey: How Recruitment is Evolving.” Resume Genius. March 17, 2025. Retrieved July 16, 2025 from [here](#)

How Hiring & HR Became a Top Target

According to Gartner Research, 84% of recruiters have experienced some form of candidate fraud.⁴ More than 75% of hiring managers report that AI makes it more difficult to assess a candidate’s authenticity.⁵ Both large and small organizations are susceptible, though the risk increases with the size of their workforce. With more employees involved, more entry points present themselves, and threat actors have more opportunities to submit modified, manipulated, or synthetic content.

Our analysis highlights five top reasons threat actors are increasingly targeting talent acquisition and human resources teams.

1. Low resistance, high value entry point

Hiring processes receive far less cybersecurity focus than corporate infrastructure. Threat actors exploit this gap, targeting recruiters and HR staff who lack training and tools to identify fraudulent candidates – making hiring workflows an unlocked “front door” that adversaries can more easily slip through.

2. Identity solutions focus on employees, not candidates

Most identity and access management security strategies focus on employees, customers, and contractors, not job seekers. Adversaries take advantage of this fact and use stolen, borrowed, or synthetic identities to pass background, identity verification, and identity proofing checks.

3. Digital-first hiring and onboarding foster deception opportunities

Continuous improvements in the quality of AI-generated digital content make it easier for imposters to appear credible. Distributed interview teams rarely regroup, making it difficult to spot red flags. Even if an imposter candidate isn’t hired, they can still gather intelligence on hiring processes for future attacks or extract sensitive information during interviews.

4. Employees working fully remote expand the attack surface

Without physical proximity, and motivated by a desire to be welcoming to a new teammate, employees are more likely to trust someone they believe is a vetted colleague. This makes them more susceptible to social engineering attacks.

5. Matrixed, global teams allow imposters to blend in

Imposter candidates tend to target Global 2000 companies because large teams spanning multiple regions, time zones, and functions make it easier for imposters to operate without raising suspicion

Why this matters: The costs of Job Candidate deception



Average organization spends \$3.7M annually on malicious insider incidents

“More than half (55%) of credential compromise incidents involved advanced social engineering (such as deep fakes or other AI-generated content).”

*Cost of Insider Risks:
Global Report 2025*

How Generative AI Threatens Digital-First Recruiting & Hiring

Threat actors submit AI-synthesized digital content throughout the hiring process to deceive recruiters, human resources staff, and interviewers. The result is hiring decisions not based in reality or a candidate's genuine qualifications.

To attract recruiters and corroborate their assumed identity, threat actors will build deceptive profiles across Facebook, professional networks (e.g., LinkedIn, Toptal), freelancer or job seeker platforms (e.g., UpWork, Freelancer.com, Freelance.com, Guru, Toptal Indeed), developer platforms (e.g., GitHub), and personal digital portfolio sites.

Adversaries then leverage generative AI to populate those deceptive profiles with AI-manipulated headshots, fabricated job histories, resumes, cover letters, code samples, and other content tailored precisely to job requirements.

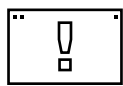
GenAI tools also support the creation of real-time audio and video deepfakes, allowing fraudsters to conceal their true identities during interviews, screening, onboarding, and daily work. This includes using AI tools to remove accents from audio in real-time, and creating deepfakes to either impersonate stolen identities or represent synthetic personas, assembled from multiple stolen or borrowed identities, on video calls.

Co-conspirators serving as references also make use of GenAI whether that's to create phony profiles or deploy real-time deepfakes to corroborate the deception.

Finally, imposters use GenAI to fabricate identity documents or manipulate photos of identity documents in order to subvert identity and employment eligibility verifications.

Imposter Hiring is a Critical Enterprise Risk

No corporation knowingly hires an individual intent on deceiving their potential employer and colleagues. Yet the consequences extend far beyond a single bad hire, introducing a multitude of risks across the organization.




Cybersecurity Risk

Hired imposters operate as trusted insiders – moving laterally through systems, harvesting credentials and data, exfiltrating sensitive information, and establishing persistent backdoor access.



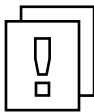
Legal, Regulatory & Compliance Risk

Hiring individuals from sanctioned nations violates U.S. and international law. It may also violate customer contracts restricting work to authorized regions. If data is stolen, the hiring organization may face regulatory penalties and mandatory breach notifications.



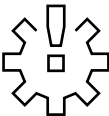
Financial Risk

Imposters send their salary along to sanctioned nation-states or criminal organizations. Some outsource their work to others while collecting multiple paychecks (i.e., overemployment). In some cases, imposters download sensitive data and demand a ransom.⁶




Intellectual Property Risk

Imposters steal trade secrets, proprietary code, and other confidential information. They may also co-opt brand assets for other deceptive purposes, potentially diluting brand integrity.



Operational Risk

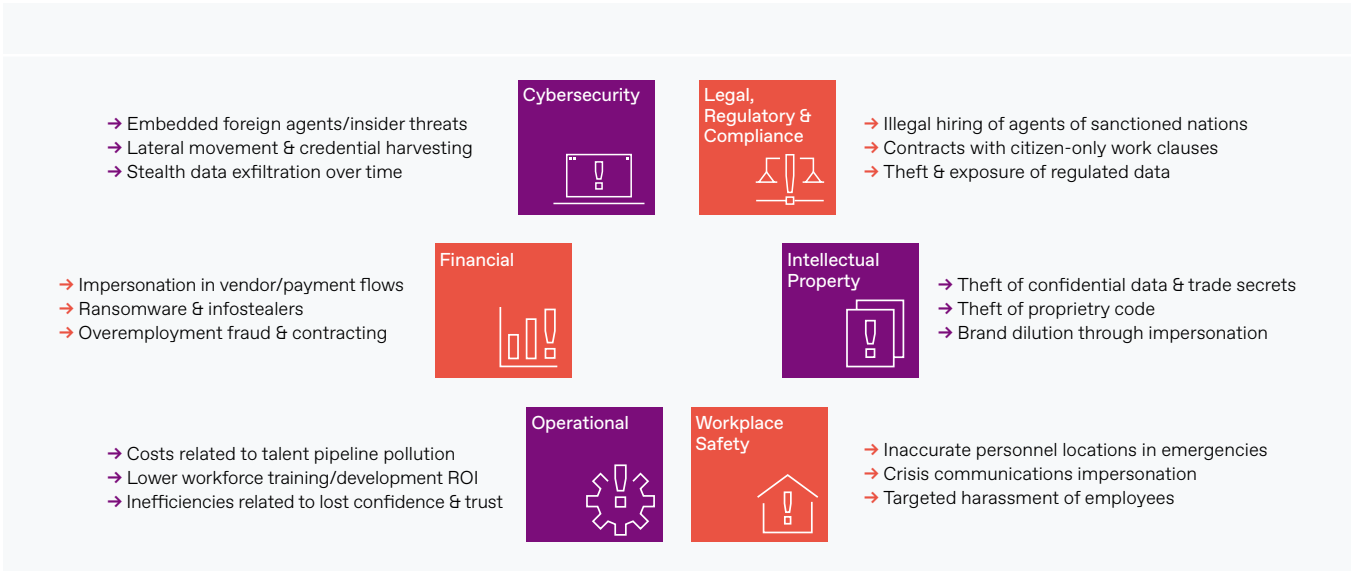
Imposters polluting the talent pipeline waste time and resources on recruiting, hiring, onboarding, and training. This degrades the candidate experience and employer brand and forces teams to repeat the entire process once an imposter is exposed.



Workplace Safety Risk

In emergencies, time spent accounting for imposters can delay response efforts. Imposters may also harass and endanger colleagues.

6 “North Korean IT Workers Conducting Data Extortion.” Retrieved June 10, 2025, from [here](#).



The Hiring Kill Chain

To help illustrate how enterprises can prevent candidate fraud up to and including the embedding of insider threats into corporate systems, we've developed the Hiring Kill Chain, inspired by Lockheed Martin's Cyber Kill Chain®.

The Hiring Kill Chain concept lays out the seven steps adversaries progress through in an attempt to get hired under false pretenses. Adopting the attacker's perspective clarifies how disrupting an adversary at any one of those points helps organizations proactively stop candidate fraud earlier.

Here we discuss each of the seven steps in brief and then dive deeper into the details and countermeasures on subsequent pages.

Hiring Process		Hiring Kill Chain	
■ OUTBOUND RECRUITING	1	CONDUCT RECONNAISSANCE	
	2	ESTABLISH IDENTITIES	
■ APPLICATION ■ SCREENING ■ INTERVIEWS ■ ASSESSMENT	3	APPLY & INTERVIEW	
■ CONDITIONAL OFFER ■ REFERENCE CHECKS ■ EMPLOYMENT ELIGIBILITY CHECKS ■ FINAL OFFER	4	CLEAR FINAL SCREENING	
■ ONBOARDING	5	COMPLETE ONBOARDING	
■ ON THE JOB	6	MAINTAIN EMPLOYMENT	
	7	EXECUTE EXIT STRATEGY	

1

Conduct Reconnaissance

Relevant Hiring Phases

→ Outbound Recruiting, prior to Application



Objective

Prior to applying for job openings, the threat actor gathers intelligence on target companies. Adversaries focus on enterprise assets and potential entry points, along with researching staff, hiring processes, and job postings. Adversaries may also identify applicant tracking systems and other HR systems (e.g., Workday, Greenhouse) used by the target for insight into taking advantage of resume filtering and screening capabilities, for example.

Hiring Process Weaknesses

- Detailed job requirements provide threat actors with a blueprint for fabricating well-fitting profiles, work histories, and resumes.

Sample Adversary Actions

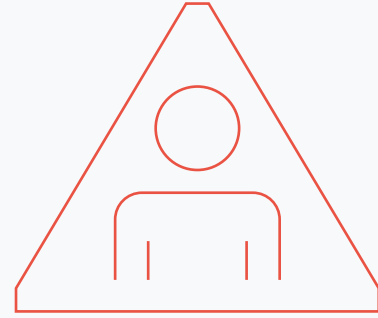
- Scrape job postings
- Research social media profiles of potential targets and staff for information about internal systems, partners, and more
- Analyze successful hires for patterns in roles, companies, and hiring processes to improve targeting.

Countermeasures

- Publish and inform job candidates of hiring process expectations explaining acceptable use of AI avatars and filters, virtual cameras, etc. to dissuade imposters
- Prescreen profiles of candidates in talent pipeline for authenticity
- Educate employees on the threat and encourage scrutiny of social media connection requests and information shared

Relevant Hiring Phases

→ Beginning prior to Application and continuing throughout the entire hiring lifecycle



Objective

Prior to applying for job openings, the threat actor builds online profiles to attract recruiters. This includes creating social media profiles built on stolen or fabricated identities and may include recruiting in-country facilitators to host laptops and accept and route payment from the employer to the threat actors once they obtain a job.

Hiring Process Weaknesses

- Recruiters over-rely on online platform profiles that can be created with minimal effort and don't require verification or use verification processes that can be subverted
- Automated HR screening tools fail to detect falsified resumes and work history
- In-depth verification of candidates' identity and work history isn't typically cost-efficient in the early stages of the hiring process
- Recruiters and HR systems lack tools and training to identify AI-generated synthetic or cloned profiles and other content

Sample Adversary Actions

- Obtain stolen identities or enlist individuals willing to share their personal information to create fraudulent job candidate profiles
- Recruit third parties to operate "laptop farms" for corporate-issued devices and to receive paychecks

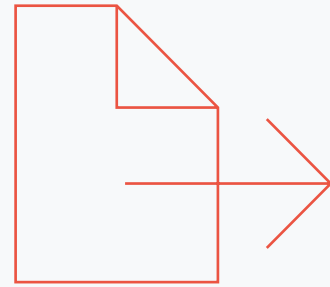
- Recruit accomplices to participate in interviews or assessments on their behalf
- Generate identity documents supporting the assumed identity
- Manipulate social media images to corroborate assumed identity (e.g., faces pasted on stock photography or other imagery suggesting presence in the U.S.)
- As needed, train AI models for generation of real-time deepfake voice and video for assumed identity
- Create online professional, freelancer, and developer profiles to attract recruiters
- Build connections (including with staff at potential targets) on online platforms
- Automatically generate resumes tailored to job postings, aligned with stolen/borrowed/synthetic identities, and optimized to pass initial screening
- Submit applications for multiple candidates to overwhelm intake and increase the odds of advancing in the talent pipeline

Countermeasures

- Brief HR and recruiting personnel and staffing agencies on the threat & require detailed candidate background information
- Verify authenticity of online, public candidate profiles
- Verify authenticity of all content submitted by candidate to identify GenAI manipulation or synthesis (and consider requiring submission of unaltered photos with candidate applications)
- Verify that phone numbers submitted by candidates are not associated with virtual phone services (e.g., Google Voice)
- Inspect resume document meta-data (e.g., PDF author) for mismatches with candidate information or signs that resumes were automatically generated
- Compare IP addresses used to submit applications against expected geography and known threat intelligence

Relevant Hiring Phases

→ Application, Screening, Interviews, Assessment and continuing throughout the entire hiring lifecycle



Objective

The imposter continues delivering fabricated digital content designed to advance through the interview stages. To sustain the illusion, imposters and their accomplices may also deploy deepfake audio and video, or stand-in interviewees throughout the process or during specific phases (e.g., technical interviews and assessments). Even without a job offer, threat actors will social engineer interviewers to collect trade secrets, competitive information, and build trust.

Hiring Process Weaknesses

- Recruiters, HR staff, and interviewers have no baseline reference to verify real-time voice or video streams, making it difficult to detect deepfakes
- Interviewers rely on facial expressions, voice, and demeanor to assess authenticity
- Lack of continual monitoring of the identity presented across the interview process allows deepfakes or stand-ins to go undetected
- Imposters may steer the conversation to extract sensitive information from interviewers

Sample Adversary Actions

- Deploy real-time deepfake audio and video during screening, interviews, and assessments to support the assumed identity
- Steer interviews to extract confidential information or trade secrets from interviewers
- Deploy real-time deepfake audio or video during proctored assessments
- Leverage AI assistants to support them in interviews and assessments
- Accomplices may use deepfake audio or video to impersonate the candidate during interviews or assessments

Countermeasures

- Track consistency of the candidate's persona throughout the application, screening, and interview processes
- Track known imposter identities, digital assets, staffing agencies, etc.
- Educate HR and recruiting agencies on the threat of imposters using real-time deepfake audio and video and ask interviewers to flag inconsistencies and suspected use of AI
- Develop and distribute a playbook for staff to follow when imposter activity or malicious genAI content is discovered in an application or during video conferencing
- Require videoconferencing for screening and prohibit virtual backgrounds
- Standardize screening questions that reveal imposters
- Monitor screening, interview, and assessment interactions for AI-manipulated, real-time audio or video
- Check IP addresses used to attend interview videoconferences or pre-employment screening for expected geography and against known threat intelligence
- Proctor assessments on your environment, disallow VPN access to assessments, and require active camera and shared screen
- Ask to meet candidates in person

4

Clear Final Screening

Relevant Hiring Phases

→ Conditional Offer, Reference Checks, Employment Eligibility Checks, and Final Offer



Objective

Upon receiving a job offer, the adversary must pass any final verification processes, such as I-9 employment eligibility verification in the U.S.

Hiring Process Weaknesses

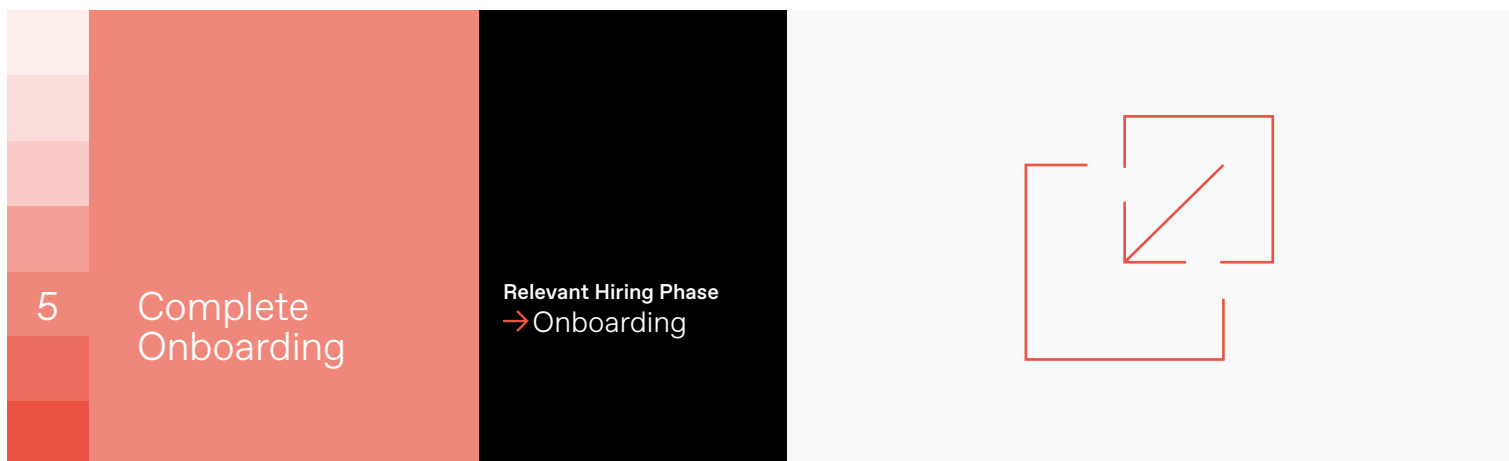
- Standard background checks are not designed to detect stolen, borrowed, or synthetic identities
- Identity verification conducted over videoconferencing can be bypassed using well-established document forgery techniques
- Digital identity verification/proofing solutions can be bypassed using deepfake identity documentation forgery and tools for subverting liveness checks
- Single point-in-time identity verification allows the imposter to continue their deception in their day-to-day, once they're verified
- HR professionals are not trained to identify sophisticated forgeries
- Candidate-provided references open the door to fake references

Sample Adversary Actions

- Submit AI-manipulated identity documents and supporting materials
- Fake references may make use of real-time deepfakes or pre-recorded deepfake audio for voicemail
- Accept offer quickly to preempt further due-diligence
- Send in-country facilitator to any requested in-person document verification meetings

Countermeasures

- Track consistency of the candidate's persona throughout the hiring process
- Screen public profiles of submitted references for authenticity
- Monitor interactions with references for AI-manipulated audio or video
- Verify that references' phone numbers are not associated with virtual phone services (e.g., Google Voice)
- Verify address and identity beyond standard background checks
- Check candidate identity against known threat actor personas
- Do not initiate candidate onboarding process until after successful completion of the ID verification process
- Build strong digital content verification and deepfake detection into document verification processes



Objective

As part of new hire onboarding, the fraudulent candidate transitions into an employee and receives credentials, system access, and trust under a false or misrepresented identity.

Hiring Process Weaknesses

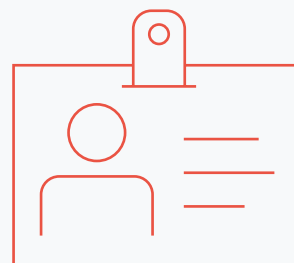
- Onboarding processes optimized for scale and speed are attended by numerous new employees allowing imposters to easily blend in
- Interview committees rarely reconvene, missing opportunities to flag inconsistencies
- Company-issued equipment sent to a candidate-provided address often does not require verification of the recipient's photo ID for delivery

Sample Adversary Actions

- Provide drop-box, "laptop farm," or mail-forwarding address for receiving corporate IT equipment
- Request last-minute changes to laptop shipping address due to a concocted emergency
- Use in-country facilitator to forward corporate IT equipment overseas
- Facilitate the receipt and configuration of corporate-issued equipment in ways that reinforce the assumed identity (e.g., setup at a laptop farm" in the expected geographic region)
- Deploy real-time deepfake audio or video during onboarding engagement as needed
- Build trust with employees and other new hires
- Research corporate assets and routes to privilege escalation

Countermeasures

- Implement start day check-ins including HR, IT, and the hiring manager to compare the new employee's live video/audio persona with interview persona and submitted ID documents
- Monitor calls to spot AI-manipulated real-time audio or video
- Monitor for atypical access – e.g., VPNs, virtual private servers (VPSs), and foreign IP addresses
- Require in-person equipment pick-up with photo ID and signature
- Compare any submitted bank account information (e.g., payee name) with identity documents



Objective

As an onboarded new hire, the adversary maintains access by performing the job adequately and continuing to conceal their true identity, qualifications, or intent. This may include outsourcing job tasks to qualified conspirators. In the case of nation-state operatives, the imposter may begin internal reconnaissance to identify assets and deepen relationships for future exploitation while maintaining cover.

Hiring Process Weaknesses

- Matrixed organizations with criss-crossing authority allow imposters to easily blend in
- Monitoring focuses on performance rather than identity assurance once credentials are provisioned
- Some victims report that imposter adversaries are top-performing employees
- Any changes in identity or contact information typically only require a corporate e-mail address for authentication

Sample Adversary Actions

- Configure tools that allow for remote management of a corporate laptop – e.g., VPNs, RMM tools (remote monitoring and management), IP KVM tools (keyboard, video, mouse over IP)
- Install hardware or software to simulate mouse activity or defeat automatic screen lock
- Maintain acceptable job performance to maintain employment and collect paychecks under false pretenses
- Outsource job tasks to co-conspirators
- Invite co-conspirators to apply for other open positions
- If needed, change address and banking information
- Deploy real-time deepfake audio or video as needed to maintain fraudulent persona
- Map internal systems and teams to target privileged users, sensitive data, and weak points

Countermeasures

- Educate employees on deepfake threats and response
- Clearly communicate acceptable use of generative AI and AI avatars to newly hired and existing employees
- Monitor for unauthorized AI-manipulated real-time audio/video
- Publish policy regarding use of RMM, KVM, third-party VPNs, and mouse activity simulation on corporate equipment
- Monitor for atypical remote employee activity (e.g., keyboard, video, mouse or “KVM” switches, RMM tools, “mouse jiggers,” and tools that defeat automatic screen lock)
- Monitor for atypical access (e.g., VPNs, foreign IP addresses)
- Validate geo-location of laptop IP address and nearby Wi-Fi access points
- Hunt for imposters/insider threats within corporate systems
- Monitor for unusual changes in direct deposit information



Objective

With internal access secured, the fraudulent candidate may seek to escalate privileges and obtain persistent access for the purposes of espionage, data exfiltration, or broader systemic attacks. They may also prepare an exit strategy in case of discovery, which can include blackmail to extort additional revenue from the enterprise.

Hiring Process Weaknesses

- Insider threats bypass traditional perimeter controls, making detection difficult
- Identities are rarely revalidated post-onboarding
- With adequate job performance, imposters can operate undetected

Sample Adversary Actions

- Exfiltrate trade secrets, competitive intel, customer data, or internal communications
- Establish backdoors or stage malware for future exploitation or retaliation

Countermeasures

- Implement least-privilege access controls
- Monitor for data exfiltration
- Approach investigations of suspected imposters carefully
 - before tipping the adversary off that they have been discovered, assess the scope of their access. Understand that if you discover one fraudulent employee, there may be others coordinating with each other

Digital Content Verification is Crucial to Disrupting the Hiring Kill Chain

Candidate fraud is a growing, global issue expected to get worse. Gartner predicts one in four job applicants will be fake by 2028.

Current hiring practices leave HR and talent teams unprepared to combat this evolving threat, especially as GenAI democratizes the synthesis of convincing resumes, identities, and personas in live interviews. No single policy or technology will solve the problem. It requires a coordinated set of controls, including identity proofing,

more diligent background and reference checks, and the ability to detect GenAI-manipulated digital content and increasingly sophisticated deepfakes throughout the hiring process.

Many organizations' hiring processes lack defenses altogether or rely on controls that are no longer up to the task of detecting today's GenAI-powered threat. Crucial weaknesses include:

→ Human judgment alone is no longer reliable

Recruiters and hiring managers can't depend solely on visual and auditory clues to detect deception. Research shows people mistake AI-generated voice content as authentically human 80% of the time.

→ Legacy checks are easily bypassed

Traditional background checks lack visual or biometric verification, which allows synthetic identities, borrowed identities, or human stand-ins to pass undetected. Background checks on stolen identities can also, typically, come back clean

→ Single point-in-time identity verification/proofing isn't fool-proof

Adversaries use manipulated or synthetic content only as needed to pass checkpoints. Synthetic or token identities, real-time deepfake audio/video, and lookalike stand-ins can all evade one-time verification. In addition, many IDV solutions do not compare identity documents against government databases in all regions, and "IDV-proof" synthetic identities are for sale on the dark web.

Many fake candidates are discovered only after they are hired, when suspicious behavior such as accessing corporate systems from unexpected IP addresses or using unauthorized remote access tools. These are important indicators but come too late.

Getting ahead of candidate fraud and imposter hiring requires a cultural and technical evolution of hiring practices:

- Equip recruiters, HR, and hiring managers with tools and training to verify digital content
- Institute continuous scrutiny of applicant-submitted content
- Implement checks on candidate artifacts such as IP addresses, email addresses, phone numbers, and social media accounts
- Move identity verification earlier in the hiring process where feasible and cost-effective
- Deploy digital content verification and real-time deepfake detection not only during recruiting and hiring, but post-hire as well

The Hiring Kill Chain focuses on prevention earlier in the hiring lifecycle, prior to compromise and HR resources being wasted.

Only by shifting security controls earlier in the hiring process will organizations achieve reliable detection of candidate deception, prevent wasted effort on fake candidates, and stop insider threats before they embed within the workforce.

7 "Predicts 2025: AI Revamps Recruitment Processes and Skills Management." Gartner. February 19, 2025. From [here](#)

8 "People are poorly equipped to detect AI-powered voice clones." Nature. March 31, 2025. Retrieved July 16, 2025 from [here](#)

Disrupt the Hiring Kill Chain

Don't let deepfakes and imposter candidates put your organization at risk. Restore trust and integrity to your hiring process with GetReal Security. To learn more and request a demo of our advanced detection solutions, visit us at

getrealsecurity.com/contact-us

About GetReal Security

GetReal Security is the cybersecurity leader specializing in the detection and mitigation of threats posed by malicious generative AI content including deepfakes and impersonation attacks. Its technology serves multinational corporations, financial institutions, media organizations, government agencies, and social media companies.

The company was incubated by Ballistic Ventures, the venture capital firm dedicated exclusively to funding and incubating entrepreneurs and innovations in cybersecurity, and Dr. Hany Farid, the preeminent expert in media forensics.