pescheck

INDUSTRY BRIEF

Personnel Screening in IT, SaaS & Cybersecurity

How technology companies can hire faster without handing the keys to the wrong person.

Saas | Cloud | Data & AI | Managed Services | Software Development

CARV | POWER APP FACTORY | Fortanix | BE DATA DRIVEN | Howspace | epilot | ABBYY

Europe's Tech Sector is Hiring at Speed into its Most Privileged Roles

In IT, SaaS and cybersecurity, almost every hire gets privileged access on day one: source code, production environments, customer tenants, admin consoles. Since NIS2's implementing regulation came into force in late 2024, cloud, managed-service and managed-security providers have an explicit legal duty to verify the background of the people in those roles. [9][10] Since November 2025, the largest cloud and platform providers serving the financial sector also fall under direct EU oversight as critical ICT third-party providers under DORA. [12]

Numbers

The talent market is straining to keep up. According to Eurostat, 57.5% of EU enterprises that recruited or tried to recruit ICT specialists in 2023 had difficulty filling those vacancies, rising above 70% in Germany and Czechia.[1] Europe faces a shortfall of more than 300,000 qualified cybersecurity professionals, with CISOs, cloud security engineers, NIS2 compliance officers and senior SOC profiles the hardest to fill.[2] Remote and freelance hiring has become the default way to close that gap, and that is exactly where the risk now sits.

North Korea's IT-worker operations have moved to Europe. In April 2025, Google's Threat Intelligence Group reported a rise in operations targeting European employers, with operatives seeking jobs in Germany and Portugal and working on projects in the UK, while posing as Italian, Ukrainian, Vietnamese and other nationals using fake and stolen identities.[3] One operative ran at least 12 personas across Europe and the US, supported by European facilitators who supplied fraudulent identity documents and helped workers get through hiring checks.[4] Google also observed workers extorting employers once they were discovered.[3]

In April 2026, the US Justice Department sentenced two facilitators of a scheme that placed North Korean workers in more than 100 US companies using at least 80 stolen identities.[5]

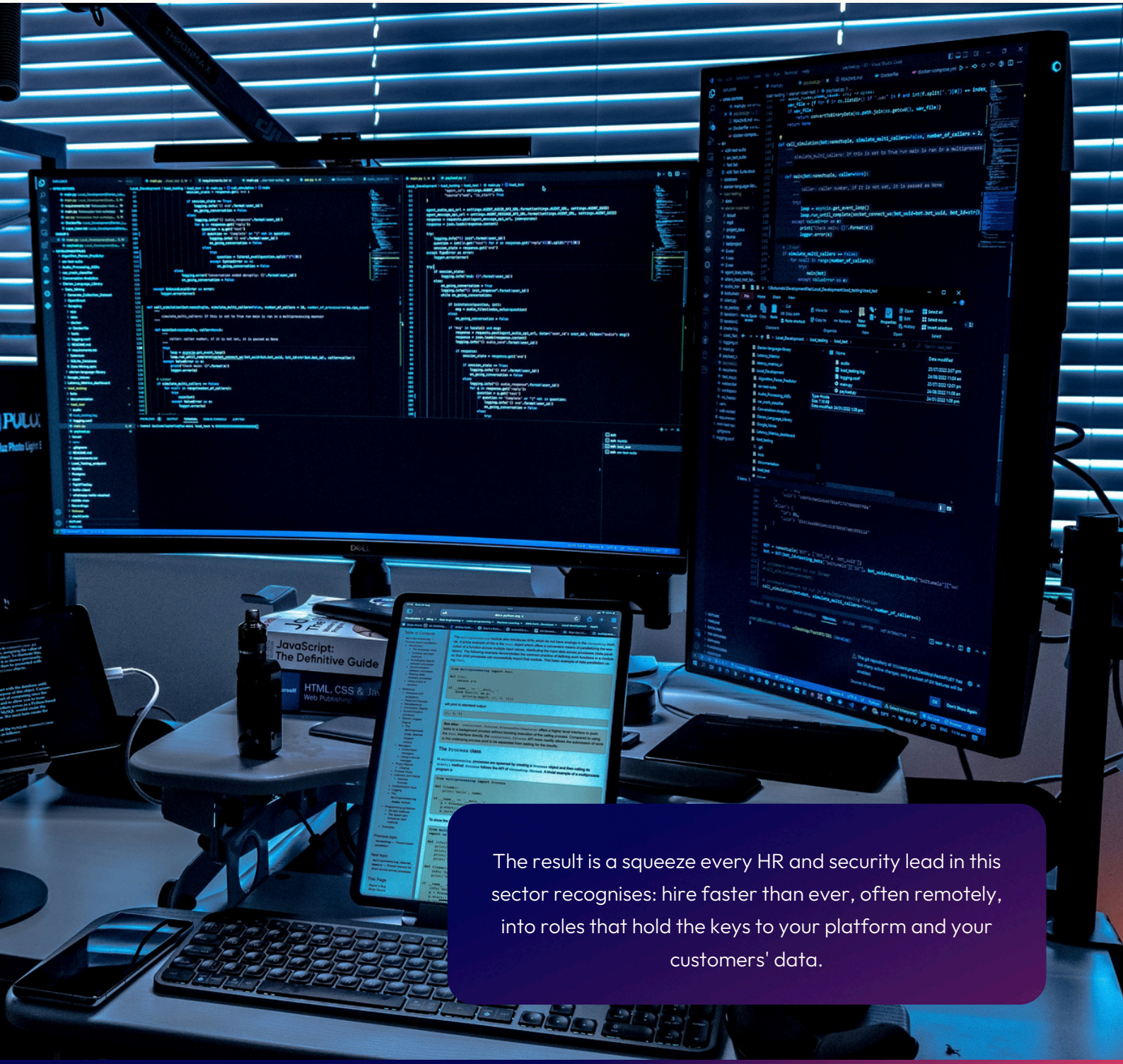
This is not theoretical for security companies either. In July 2024, KnowBe4, a security-awareness vendor, disclosed that a newly hired principal software engineer was a North Korean operative using a stolen US identity. He had passed four video interviews, reference checks and a background check, and began loading malware the moment his company laptop arrived.[6]

Criminal groups now recruit insiders directly. In 2025, a representative of the Medusa ransomware gang offered a BBC correspondent 15% of any ransom, later raised to 25%, in exchange for access to his employer's systems, and flooded his phone with MFA prompts when he stalled.[7] The control that matters in these cases is identity and integrity verification at the point of hire and during employment, not the firewall.

pescheck

The Candidate Side of the Market

The candidate side is shifting too. In a 2025 Gartner survey of 3,000 job candidates, 6% admitted to interview fraud, either posing as someone else or having someone else pose as them. Gartner predicts that by 2028, one in four candidate profiles worldwide will be fake, and warns that candidate fraud creates cybersecurity risks far more serious than a bad hire.[8] Deepfaked video interviews, AI-written CVs and borrowed identities hit tech employers first, because their roles are remote, well paid and come with privileged access.



The result is a squeeze every HR and security lead in this sector recognises: hire faster than ever, often remotely, into roles that hold the keys to your platform and your customers' data.

Why Screening is Now a Compliance Requirement, not a Nice-to-Have

For software, cloud, managed-service and cybersecurity companies, personnel screening sits at the intersection of several regimes at once, some binding directly and some arriving through customers:

- **NIS2 and Implementing Regulation (EU) 2024/2690.** Article 21(2)(i) of NIS2 makes human resources security a cybersecurity risk-management measure. The implementing regulation applies specifically to cloud computing, data centre, managed service and managed security service providers, among other digital providers.[9] Its point 10.2 requires them to verify, to the extent feasible, the background of employees, and where applicable of direct suppliers and service providers, where the role requires it, and to define which roles may only be held by verified people.[10]

- **DORA, for ICT providers to financial services.** Banks, insurers and payment firms must manage the risk of their ICT providers, and their HR policies must cover the provider staff who access their ICT assets.[11] That obligation flows down into contracts and audits of SaaS and IT vendors. In November 2025, the European Supervisory Authorities designated the first 19 critical ICT third-party providers, including AWS, Google Cloud, Microsoft, Oracle, SAP and Deutsche Telekom, which are now under direct EU oversight. [12]

- **ISO/IEC 27001:2022, control A.6.1.** Background verification must be carried out on all candidates before joining and on an ongoing basis, proportional to the classification of information accessed and the perceived risks.[13] Auditors expect a screening policy, a role risk-classification matrix and a documented screening record per person.

- **SOC 2.** The framework does not prescribe specific checks, but under criterion CC1.4 auditors routinely sample new hires and test background-check records, and expect access to be granted only after screening is complete.[14]

- **Government and defence customers.** Public-sector contracts, national security clearances and customer-imposed requirements for staff working on sensitive tenants or classified projects each add their own documentation burden.

- **GDPR.** All of the above must be lawful, data-minimised and defensible, with particular care around criminal-record data under Article 10, especially when screening contractors and freelancers in several countries.

PESCHECK helps technology companies translate security and compliance requirements into consistent, role-based screening workflows across countries, entities and contractor networks.

Matching Screening Depth to Role Risk



Screening depth: Standard

Frontend developer at a SaaS scale-up

This developer works on the product's codebase and internal tools, but has no standing access to production data or customer tenants. The main risks are a misrepresented identity or skill set, including fake remote candidates, and source code or IP leaving with a departing employee.

Screening: identity and biometric verification, education verification, employment history, references, a VOG with a role-appropriate screening profile, and a sanctions check.



Screening depth: Privileged

Cloud or DevOps engineer at a managed service provider

Holds admin rights across customer environments, CI/CD pipelines and production infrastructure. The key risks are a fake or proxy identity, insider recruitment, and undisclosed conflicts of interest. Under NIS2's implementing rules, this is the role that should be held by a verified person.

Screening: the standard package, plus an adverse media check, an integrity and conflict-of-interest declaration, international criminal record checks for previous countries of residence, verification that the person interviewed is the person onboarded, and periodic re-screening.



Screening depth: Enhanced

Security analyst or incident responder at an MSSP

This person sees clients' vulnerabilities, detection logic and incident data, and may work on classified or sovereign-cloud environments. The key risks are hostile-state recruitment, misuse of client intelligence, and undisclosed foreign ties.

Screening: the privileged package, plus in-depth sanctions and PEP screening, extended references from previous security employers, documentation that supports a national clearance where the customer requires one, and, where lawful and proportionate, a financial check.

What is Actually Possible to Verify

A well-designed programme starts from the risk, not the check. Every role carries a baseline risk of misrepresented identity, qualifications or work history. Privileged roles add exposure to insider recruitment and conflicts of interest. Security and government-facing roles add sanctions exposure and undisclosed foreign ties.

Each tier therefore gets a different depth of screening, matched to what could actually go wrong in that role. Pescheck supports the full range, from standard verification to in-depth checks for the most sensitive positions.[15]

- Identity fraud → Identity & biometric verification
- Insider / integrity risk → Integrity declaration, adverse media
- Export-control exposure → Relevant declarations and documentation
- Qualification risk → Education and certification verification
- Experience risk → Employment and reference verification
- Sanctions exposure → Sanctions / PEP / watchlist screening
- Ongoing personnel risk → Periodic or event-based re-screening

The Pescheck Case

The challenge our customers brought us

- Fully remote and cross-border hiring, with candidates and contractors in many countries and few in-person touchpoints
- High hiring volume in engineering, cloud operations and support, often through agencies and freelance platforms
- Manual, decentralised screening that differed by team and did not scale with growth
- Enterprise and public-sector customers demanding evidence of personnel security in security questionnaires and audits
- Compliance obligations spanning NIS2, ISO 27001, SOC 2 and customer DORA requirements simultaneously

What we implemented

- Standardised screening workflows per role tier, so the same evidence is collected the same way in every country, entity and contractor network
- Identity-first check packages with biometric verification to stop fake and proxy candidates before they receive a laptop or credentials
- ATS and HR system integration, alongside 100+ other integrations and a full API, so screening starts automatically from the existing recruitment process [15]
- Centralised dashboard with live status per candidate, structured decision-making and a complete audit trail that maps directly to ISO 27001 and SOC 2 evidence requests
- EU-built, EU-hosted infrastructure, ISO 27001 and NEN 7510 certified, POB/WPBR registered and PBSA affiliated [16]

The outcome

- Designed to support a compliant, audit-ready screening process, with each step documented so decisions can be explained to auditors, customers and regulators
- Average turnaround of under 4 hours, so screening never becomes the reason an engineer accepts another offer[15]
- A consistent screening standard across teams, entities and countries, including contractors
- More than 300,000 screenings performed on our technology for 2,600+ organisations[15]

Why it Matters Commercially, not Just Legally

Screening is increasingly a condition of winning deals in this sector. Enterprise security questionnaires ask how staff with access to customer data are vetted, ISO 27001 and SOC 2 auditors sample hiring records, financial-services customers push DORA requirements down to their vendors, and public-sector tenders ask for screened or cleared staff. At the same time, you need to hire scarce engineers quickly, before they accept another offer. PESCHECK sits exactly between those two needs. A documented, standardised programme keeps hiring moving and turns a compliance cost into an answer you can put in every security questionnaire.

The economics hold up independently. Around 10% of candidates show a background discrepancy, and a bad hire can cost up to 2.5x their salary,[15] before accounting for a lost enterprise deal or a breached customer. At the extreme end, breaches started by malicious insiders are the costliest initial attack vector, averaging $4.92 million per incident.[17] Speed matters, but not at the expense of security.

Organisations in this sector working with Pescheck include [customer names to confirm - e.g. SaaS companies, MSPs/MSSPs, cloud and hosting providers, security vendors].

ABBYY | Howspace | epilot | FTAPI | CARV | POWER APP FACTORY | Fortanix | BE DATA DRIVEN



Sources

1. Eurostat, ICT specialists – statistics on hard-to-fill vacancies in enterprises — 57.5% of recruiting EU enterprises had difficulty filling ICT vacancies in 2023; Germany 72.4%, Czechia 70.5%.

2. Optima Europe, European Cybersecurity Talent Market 2026 — shortfall of 300,000+ cyber professionals; hardest-to-fill roles.

3. The Record, North Korean IT worker scam spreading to Europe after US law enforcement crackdown (April 2025), reporting Google Threat Intelligence Group — Germany, Portugal, UK; false nationalities; extortion.

4. Help Net Security, North Korean IT workers set their sights on European organizations (April 2025) — one operative with 12+ personas; European facilitators supplying fraudulent IDs.

5. The Hacker News, Researchers built a fake crypto startup and hired three suspected North Korean IT workers (August 2026) — references April 2026 sentencing of two facilitators; 100+ companies; 80+ stolen identities.

6. SecurityWeek, KnowBe4 hires fake North Korean IT worker, catches new employee planting malware (July 2024); see also KnowBe4's incident FAQ — stolen US identity; four video interviews; background check passed.

7. BleepingComputer, Ransomware gang sought BBC reporter's help in hacking media giant (September 2025) — Medusa offered 15%, later 25%, of ransom for insider access.

8. Gartner, Survey shows just 26% of job applicants trust AI will fairly evaluate them (July 2025) — 6% admitted interview fraud; 1 in 4 candidate profiles fake by 2028.

9. ENISA, Implementing guidance on Commission Implementing Regulation (EU) 2024/2690 — scope: cloud, data centre, MSP, MSSP and other digital providers.

10. Cyberday, NIS2 Implementing Regulation 10.2: Verification of background — text of points 10.2.1 and 10.2.2.

11. Springlex, DORA RTS on ICT risk management (CDR (EU) 2024/1774), Article 19 – Human resources policy — covers ICT third-party provider staff with access to ICT assets.

12. EBA, ESAs designate critical ICT third-party providers under DORA (18 November 2025); list summarised by PayTechLaw — 19 CTPPs.

13. ISMS.online, ISO 27002:2022 Control 6.1 – Screening.

14. CertPro, SOC 2 controls: full list, categories and how they are tested — CC1.4: auditors test background-check records.

15. Pescheck, platform capabilities and figures — 100+ integrations and API, <4h average turnaround, 300,000+ screenings, 2,600+ organisations, ~10% discrepancy rate, bad hire up to 2.5x salary (figures carried over from the defence brief; confirm before publishing).

16. Pescheck, certifications — ISO 27001, NEN 7510, POB/WPBR, PBSA (replace with an IT/tech industry page if one exists).

17. IBM / Ponemon, Cost of a Data Breach Report 2025, summarised by Baker Donelson — malicious insider attacks the costliest initial vector ($4.92m).