THE QUESTION EVERY PARENT IS ASKING

Will cybersecurity still be a career when my kid grows up?

AI agents now triage security alerts, write phishing emails, and even run parts of real cyberattacks. So is telling a 12-year-old to pursue cybersecurity still good advice, or are we pointing them at a field that machines will hollow out before they graduate? **Here is what the actual data says.**

> **OUR PROMISE:** No fairytale, no doom. Every number below is labeled by what it really is: measured data, a vendor's marketing claim, or a forecast. Where the evidence is uncomfortable, we print it anyway.

MEASURED DATA · VENDOR CLAIM · PROJECTION

Published by ROOT ACCESS · Sources: BLS, ISC2, CyberSeek/NIST, Lightcast, SANS, Gartner, WEF, IBM, Stanford. Full citations at the end.

PART 1 · WHAT'S ACTUALLY HAPPENING

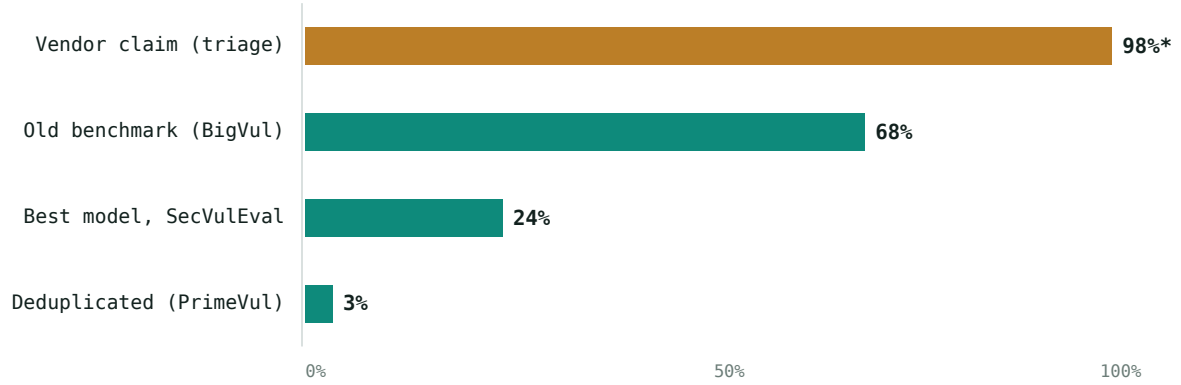
The robots really are in the security room

This isn't hypothetical. AI "agents" (software that acts on its own, not just chats) are already working inside security operations centers (SOCs), the 24/7 teams that watch for attacks. Tampa's own ReliaQuest markets its platform as automating **98% of security alerts** and says it "eliminates Tier 1 and Tier 2 security operations work,"[13] which is exactly the work beginners have traditionally been hired to do. VENDOR CLAIM

CrowdStrike claims its Charlotte AI triages detections with "over 98% accuracy," saving analysts 40+ hours a week,[12] VENDOR CLAIM though "accuracy" there means matching CrowdStrike's *own* analysts, not an outside audit. And the attackers have agents too: in November 2025, Anthropic disclosed the first documented large-scale AI-orchestrated espionage campaign, in which AI performed an estimated **80 to 90% of the tactical work** across roughly 30 targets.[11] MEASURED DATA

Marketing vs. the lab bench: how good is security AI, really?

VENDOR-CLAIMED ACCURACY VS. INDEPENDENT ACADEMIC BENCHMARKS (F1 SCORE)



*CrowdStrike's 98% measures agreement with its own analysts on routine triage, a real but narrow task.[12] When independent researchers test AI on deep security reasoning, results collapse: the same class of models that scored 68% on an older, contaminated benchmark scored just 3% (F1) once the dataset was cleaned (PrimeVul), and the best frontier model managed 24% on SecVulEval's real-world vulnerability analysis.[14] AI is genuinely good at the routine layer, and still bad at the judgment layer.

Practitioners see the gap. In the SANS 2025 SOC Survey, working analysts ranked AI/ML tools **at the bottom** of their satisfaction list.[9]

MEASURED DATA Gartner predicts **over 40% of agentic-AI projects will be canceled by the end of 2027**, and estimates only about 130 of the thousands of "agentic AI" vendors are actually agentic.[8] PROJECTION

Why is AI being adopted anyway? Because the humans were drowning. SOC teams receive an average of **3,832 alerts per day and ignore 62% of them**;[10] 71% of analysts report burnout.[10] MEASURED DATA AI isn't (yet) replacing great analysts. It is absorbing the flood that entry-level analysts used to be hired to bail out.

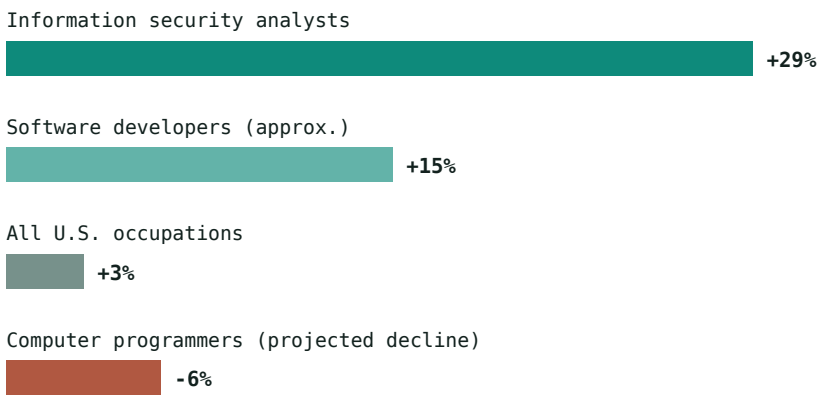
PART 2 · THE DEMAND PICTURE

The field is still growing, fast

Set the AI question aside for a moment. Is anyone still hiring? Yes, at nearly ten times the pace of the average job. The U.S. Bureau of Labor Statistics projects information-security-analyst employment to grow **29% from 2024 to 2034**: the fifth-fastest-growing occupation in America, with about 16,000 openings a year.[1] PROJECTION

Projected job growth, 2024-2034

U.S. BUREAU OF LABOR STATISTICS · SELECTED OCCUPATIONS



Cybersecurity is a relative winner even *inside* tech: BLS projects some adjacent computer occupations to shrink as automation advances, while security keeps growing.[1] BLS itself cautions its model does not fully price in AI disruption.

514,359

U.S. cyber job postings in the 12 months ending April 2025, up 12% year over year

CYBERSEEK · MEASURED[3]

74%

supply-demand ratio: only enough workers to fill about 3 of every 4 open roles

CYBERSEEK · MEASURED[3]

$124,910

median pay for information security analysts (May 2024)

BLS · MEASURED[1]

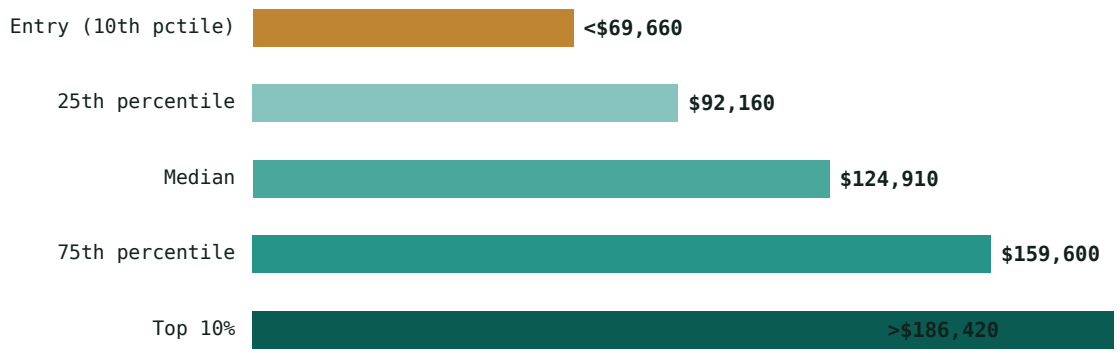
$10.22M

average cost of a U.S. data breach in 2025, a record and the reason demand won't vanish

IBM · MEASURED[6]

The pay ladder: where the money actually lives

INFORMATION SECURITY ANALYST ANNUAL WAGES, MAY 2024 · BLS



The spread from under $70K (entry) to over $186K (senior) tells the story of the next decade: compensation growth lives in **experience and specialization**, exactly the tier AI is not replacing.[1] The amber bar is the rung under pressure.

PART 3 · THE UNCOMFORTABLE PART

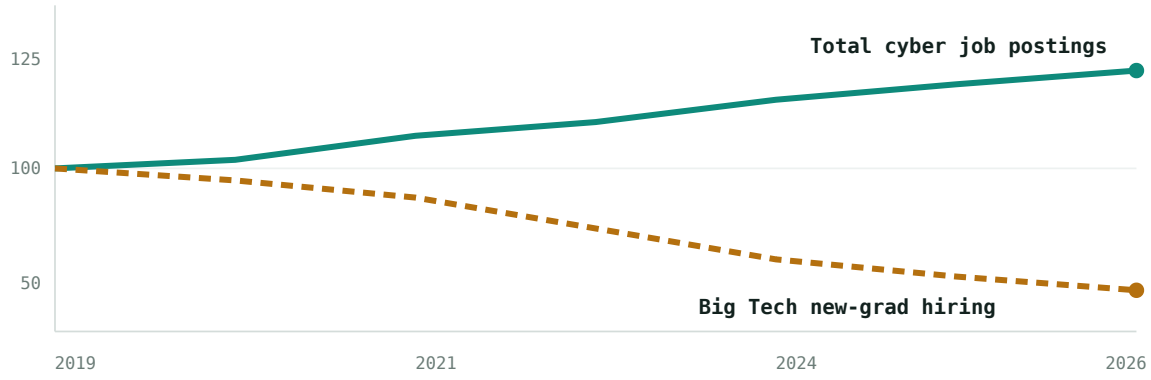
The front door is narrowing

Here is the part a fairytale would skip. The shortage in cybersecurity is a shortage of **experienced** people, not beginners. Lightcast found entry-level cyber roles (0-2 years) actually had a worker **surplus of roughly 10 to 12%**, while roles needing 2+ years had only 76% of the supply required.[4] MEASURED DATA

And organizations are hiring fewer beginners at all. In ISC2's 2025 workforce study, **31% of organizations reported having zero entry-level security staff**; among large organizations, 49% reported hiring freezes and 32% reported layoffs. Tellingly, ISC2, which spent years publicizing a "4-million-job workforce gap," **stopped publishing the gap number entirely in 2025**, reframing the problem as a skills gap.[2] MEASURED DATA

The squeeze: total demand up, beginner access down

ILLUSTRATIVE INDEX, 2019 = 100 · BUILT FROM CYBERSEEK, LIGHTCAST & SIGNALFIRE TRENDS



Directionally accurate, not to scale. Cyber postings grew about 12% in the year to April 2025 alone,[3] while SignalFire measured Big Tech new-grad hiring down 25% in 2024 and **more than 50% below 2019 levels**, re-accelerating downward in 2026.[5] This is the leading indicator cyber entry roles historically follow, and this one picture is the whole report.

Is AI the cause? The best early evidence says it's a real contributor: Stanford's "Canaries in the Coal Mine" study found a **13% relative employment decline for workers aged 22 to 25 in the most AI-exposed occupations**, concentrated where AI *automates* rather than assists, and statistically significant from 2024 onward. [7] MEASURED DATA (The authors caution it's correlational, and interest rates and the tech slowdown share blame.)

> **The shortage is real. It's just not a shortage of beginners, and AI is automating the exact job beginners used to be hired for.**
>
> THE HONEST ONE-SENTENCE SUMMARY OF 2026

PART 4 · THE DECADE TRACE

Follow one kid: age 12 today, first job in 2036

Meet a 7th grader starting the school year in fall 2026. Call them Alex. Alex will finish high school in **2032** and enter the workforce around **2036**, the exact far edge of every projection in this report. Here is Alex's path, stage by stage, next to what the data says the industry will look like at each moment. (Every program named is real, free or low-cost, and age-appropriate.)

2026 TO 2028 · MIDDLE SCHOOL · AGE 12-14

Curiosity, safely

WHAT ALEX DOES

- **Play, don't grind:** CyberPatriot (middle-school division), picoCTF's practice gym at 13+, Scratch then Python.
- Learn AI as a *tool*: using it, questioning it, spotting when it's wrong.
- In Florida: free Cyber Florida student camps and school clubs.

THE WORLD THEN

- Gartner: 40%+ of agentic-AI projects **canceled by end of 2027**. The hype cycle shakes out while Alex is in 8th grade.[8]
- Tier-1 triage automation spreads through SOCs; alert-drowning (62% ignored today[10]) fades as the human problem.

2028 TO 2032 · HIGH SCHOOL · CLASS OF 2032

Build proof, not just grades

WHAT ALEX DOES

- Cyber/CS electives plus dual enrollment; earns a first industry cert (e.g., Security+). In Florida, CAPE certifications even earn their teacher a bonus and the school funding.
- Competes: CyberLaunch (free, statewide), picoCTF, National Cyber League (about $45/season).
- Builds a home lab and a public portfolio; applies to a high-school internship (Tampa's ReliaQuest runs one).

THE WORLD THEN

- Gartner: by 2028, GenAI removes the need for specialized education in **50% of entry-level cyber jobs**; aptitude and demonstrated skill beat credentials.[8]
- WEF: by 2030, **39% of core job skills change**; security is a top-3 fastest-growing skill; net **+78M jobs** globally.[15]
- Gartner: half of enterprise incident response involves **AI applications** by 2028, a brand-new job category forming while Alex is a sophomore.[8]

2032 · THE LAUNCH DECISION · AGE 18

Three doors, not one

WHAT ALEX CHOOSES BETWEEN

- **Degree route:** a cyber/CS program (e.g., USF's AI + cybersecurity college) with mandatory internships, possibly on a service scholarship (CyberCorps SFS, NSA Stokes: tuition paid, job guaranteed).
- **Earn-while-learning:** registered cyber apprenticeships, including the DoD's no-experience-required paid apprenticeship: get paid, get cleared, convert to a federal career.
- **Stacked route:** community college plus certs plus help desk, climbing inside a company.

THE WORLD THEN

- The "get one cert, walk into a SOC seat" path is largely gone; hybrid AI-fluent skills are the baseline.
- Students have already rotated: CS enrollment fell more than 10% in 2025-26 while cyber and AI programs *grew*, so Alex faces less naive competition and better-defined pathways.[16]

2032 TO 2036 · POSTSECONDARY · AGE 18-22

Specialize where AI is weak

WHAT ALEX DOES

- Picks a durable lane: AI security / MLSecOps, detection engineering, incident response, OT and critical infrastructure, or AI governance and GRC.
- Treats AI agents as staff to be **supervised, audited, and red-teamed**: the "human on the loop."
- Stacks internships and apprenticeship hours; considers a clearance, a uniquely automation-proof and offshore-proof credential. Tampa Bay, with MacDill AFB and its contractor ecosystem, is one of the best places in America to get one.

THE WORLD THEN

- BLS's +29% growth window (2024-2034) closes with Alex mid-college, and openings ran about 16,000/year through it.[1]
- Attack surface keeps compounding: record breach costs ($10.22M avg. U.S., 2025[6]) and documented AI-run attacks[11] keep budgets flowing to defense.

APPROX. 2036 · FIRST FULL-TIME ROLE · AGE 22-23

Alex's first job (it isn't alert-watching)

WHAT THE JOB LOOKS LIKE

- Titles like **AI security engineer, detection engineer, incident responder, AI-governance analyst**: supervising fleets of security agents, investigating what they escalate, hunting what they miss.
- Entry pay in today's dollars: high $60Ks to about $90K, with a documented ladder to $125K (median) and $186K+ (senior).[1]
- The humans AI can't replace: judgment, adversarial creativity, and someone accountable when it matters.

THE HONEST ODDS

- Ten years of evidence says the field **transformed rather than vanished**, as happened before to NOC operators, IT help desks, and QA testers, whose fields shifted upward and mostly grew.
- The kids who struggled are the ones who trained for 2024's entry-level job. Alex trained for 2036's.

PART 5 · WHERE THE JOBS MOVE

Shrinking rungs, growing branches

Security role	10-year outlook	Why
Tier-1 SOC analyst (alert triage)	COMPRESSING	The explicit automation target; vendors advertise "eliminating Tier 1 and Tier 2 work."[13]
Routine log review / first-pass phishing analysis	COMPRESSING	High-volume and pattern-based, precisely what agents do well.
Pen tester (routine scans)	SPLITTING	Automated discovery grows (Google's AI found 20 real vulnerabilities in 2025[14]); creative adversarial work stays human.
GRC / compliance	GROWING	EU AI Act, NIS2, and SEC rules create AI-governance work that requires accountable humans.
Detection engineer / threat hunter	GROWING	Someone must build, tune, and out-think the automated defenses.
Incident responder / commander	GROWING	Judgment under fire, legal weight, accountability: AI's weakest ground.
AI security engineer / MLSecOps / AI red-teamer	NEW & GROWING	Securing the AI itself is a net-new field. Gartner: half of enterprise IR involves AI apps by 2028.[8]
OT / critical infrastructure and cleared defense work	RESILIENT	Physical stakes, regulation, and clearances make it automation-resistant and offshore-resistant. Tampa Bay's home-field advantage.

PART 6 · THE COMPARISON PARENTS ACTUALLY MAKE

Compared to what?

No career is AI-proof. The fair question is whether cybersecurity is more or less exposed than the paths parents weigh against it. Four structural shields set cyber apart: it faces a **live adversary** that adapts to every automation (a permanent arms race; AI attacking[11] creates demand for AI-era defenders); it is increasingly **regulated**, and regulations require accountable humans; a breach carries **legal liability** no company will pin on an unsupervised bot; and a large slice of the work is **clearance-gated**, so it cannot be automated offshore or handed to an uncleared model.

Path	AI exposure	The one-line read
Cybersecurity	LOWER (shielded)	The routine tier automates; adversary, regulation, and liability keep growing the human layer. BLS: +29%.[1]
Software engineering	MODERATE TO HIGH	Code generation hits juniors hardest; new-grad hiring already down 50%+ from 2019.[5]
Accounting / bookkeeping	HIGH	Rule-based and document-heavy, squarely in automation's lane, with no adversary fighting back.
Paralegal / legal research	HIGH	Research and drafting are core LLM strengths; the profession's entry layer is thinning.
Skilled trades / nursing	LOW	Physical-world work stays hardest to automate, the honest benchmark for "AI-safe."

Students have noticed: while overall CS enrollment fell more than 10% in 2025-26, cybersecurity and AI programs grew.[16] MEASURED DATA

PART 7 · THE VERDICT

What we'd tell a parent, straight

Yes: cybersecurity remains one of the better bets a young person can make. But the advice has changed. Ten years ago the pitch was "millions of unfilled jobs; get a cert and you are in." That pitch is dead; the organization that invented the number stopped publishing it.[2] The 2026-and-beyond version is: **enter through proof and pipelines, not postings**. That means competitions, portfolios, internships, and apprenticeships, aimed from the start at the work AI can't own: judgment, adversarial creativity, supervising the machines, and being the accountable human.

IF AI PLATEAUS (AGENTS STAY UNRELIABLE)

The Tier-1 job partially survives; demand stays hot; today's playbook still wins. Evidence for: benchmark failures, SANS satisfaction rankings, Gartner's 40% cancellation call.[8][9][14]

THE MIDDLE PATH (MOST LIKELY)

Routine work automates; total demand grows in changed form; entry stays hard but pipelines widen. Every prior automation wave in adjacent IT fields landed here.

IF AI LEAPS (RELIABLE END-TO-END AGENTS)

Entry contracts sharply and the mid-tier squeezes; the durable humans are architects, AI-governors, IR commanders, and cleared personnel. Even here, cyber fares better than most white-collar fields, because the attackers have agents too.[11]

The parent playbook

Do

- Start free and early: CyberPatriot, picoCTF (13+), Cyber Florida programs. Play before pressure.
- Make AI fluency non-negotiable: using it, questioning it, and eventually auditing it.
- Collect proof: home labs, CTF results, a public portfolio, dual-enrollment credits, a first cert in high school.
- Target pipelines: internships, registered apprenticeships, service scholarships (tuition for service), help-desk ladders.
- In Tampa Bay, use the home field: MacDill's contractor ecosystem, USF's AI + cyber college, ReliaQuest's student programs, and consider the clearance path.

Don't

- Don't repeat the "millions of unfilled jobs" pitch; it is retired, and believing it sets kids up for a shock.[2]
- Don't bank on a single certificate as a golden ticket, or train a kid to be an alert-watcher; that is the job being automated.[13]
- Don't panic-swerve away from tech entirely; the data says cyber is among the *more* resilient options.
- Don't take vendor "98% accuracy" claims, or this report's projections, as settled fact. Re-check yearly; we do.

What would change our advice: if BLS cuts cyber growth below about 15%, if CyberSeek's supply ratio climbs past about 90% (the gap closing), or if *independent* tests show agents reliably running end-to-end investigations above 90%, we will say so. That's the deal.

Sources & citations

1. **U.S. Bureau of Labor Statistics**, Occupational Outlook Handbook: Information Security Analysts (2024-2034 projections; May 2024 wage data). bls.gov/ooh
2. **ISC2 Cybersecurity Workforce Studies**, 2024 and 2025 (workforce gap discontinued 2025; entry-level staffing, hiring freezes, layoffs; released Dec 4, 2025). isc2.org
3. **CyberSeek** (NIST NICE / CompTIA / Lightcast), data update June 2, 2025: 514,359 postings; 74% supply-demand ratio. cyberseek.org
4. **Lightcast**, Cybersecurity Talent Reports 2024: entry-level surplus vs. experienced shortfall; AI-skill posting share rising from 6.3% to 9.6%. lightcast.io
5. **SignalFire**, State of Talent Reports 2025 and 2026: Big Tech new-grad hiring down 25% (2024), more than 50% below 2019; decline re-accelerating. signalfire.com
6. **IBM**, Cost of a Data Breach Report 2025: $4.44M global / $10.22M U.S. average; AI and automation savings of $1.9M. ibm.com
7. **Stanford Digital Economy Lab** (Brynjolfsson, Chandar, Chen), "Canaries in the Coal Mine," Aug 2025 (updated Feb 2026): 13% relative decline, ages 22 to 25, AI-exposed occupations. digitaleconomy.stanford.edu
8. **Gartner**: agentic-AI cancellations above 40% by 2027 (June 25, 2025); GenAI removing the specialized-education need in 50% of entry-level cyber jobs by 2028; 50% of enterprise IR involving AI applications by 2028 (Mar 2026). gartner.com
9. **SANS Institute**, 2025 SOC Survey (444 respondents; AI/ML tools ranked last in satisfaction) and 2025 AI Survey. sans.org
10. **Vectra AI**, State of Threat Detection 2024 (3,832 alerts/day; 62% ignored); **Tines**, Voice of the SOC Analyst (71% burnout). vectra.ai / tines.com
11. **Anthropic**, disclosure of the GTG-1002 AI-orchestrated espionage campaign, Nov 13, 2025: AI executed roughly 80 to 90% of tactical operations across about 30 targets. anthropic.com
12. **CrowdStrike**, Charlotte AI Detection Triage (GA Feb 13, 2025): vendor-claimed 98%+ accuracy vs. an internal analyst baseline. crowdstrike.com *(vendor claim)*
13. **ReliaQuest** (Tampa, FL), GreyMatter agentic AI announcements 2024-2025: vendor-claimed 98% alert automation; "eliminates Tier 1 and Tier 2 work." reliaquest.com *(vendor claim)*
14. **Independent benchmarks**: PrimeVul (deduplicated; F1 collapse to about 3%), SecVulEval (best model 23.8% F1), VulDetectBench; Google Project Zero "Big Sleep" (20 vulnerabilities, Aug 2025). arXiv / googleprojectzero

15. **World Economic Forum**, Future of Jobs Report 2025: 170M created / 92M displaced / net +78M by 2030; 39% of core skills changing. weforum.org
16. **Goldman Sachs** (June 2026) and **National Student Clearinghouse** (fall 2025): CS enrollment declines of more than 10% / 8.1% (CS 11.2%) while cybersecurity and AI programs grew; CRA CERP Pulse Survey Oct 2025.

ROOT_ACCESS // FIELD REPORT · Compiled July 2026 · Tampa Bay, Florida
Honesty notes: vendor accuracy figures are self-reported marketing metrics, not independent audits. Projections (BLS, Gartner, WEF) are forecasts with uncertainty, not guarantees. The Stanford finding is correlational. The widely quoted "$10.5 trillion cybercrime cost" does not appear in this report because its methodology is contested. All figures are re-verified on the ROOT ACCESS bi-weekly maintenance cycle; if the data changes, this report changes.