

# **NICE Webinar - Preparing Tomorrow's Workforce: Insights into Cyber Workforce Trends**

---

March 18, 2026

# Notes and Reminders



**Attendees are muted:** Due to the number of attendees, all participant microphones and cameras are automatically muted.



**Webinar Recording:** This webinar and the engagement tools will be recorded. An archive will be available at [www.nist.gov/nice/webinars](http://www.nist.gov/nice/webinars).



**Submitting Questions:** Please enter questions and comments for presenters in the Zoom for Government Q&A. Chat has been disabled for this event.



**CE/CPE credits:** The CEU form will be available on the event page after the event.



Karen Wetzel

*National Institute of  
Standards and  
Technology*



Brian Correia

*SANS | GIAC*



Will Markow

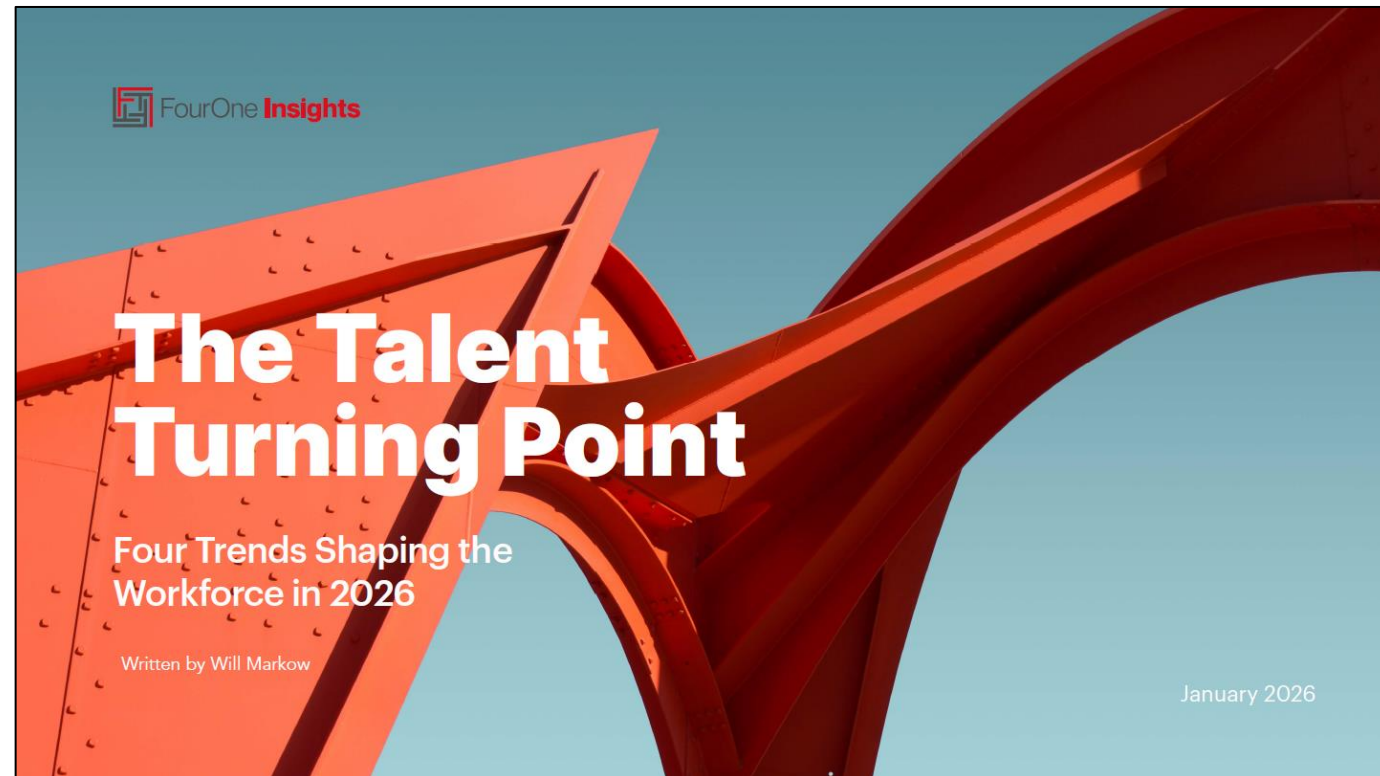
*FourOne Insights*



# Future-Proofing the **Cybersecurity Workforce**

**Will Markow**  
Founder and CEO

# What Trends are Shaping the Future of the Workforce?



# The Vanishing Career Ladder

Will Entry-Level Jobs Rebound?

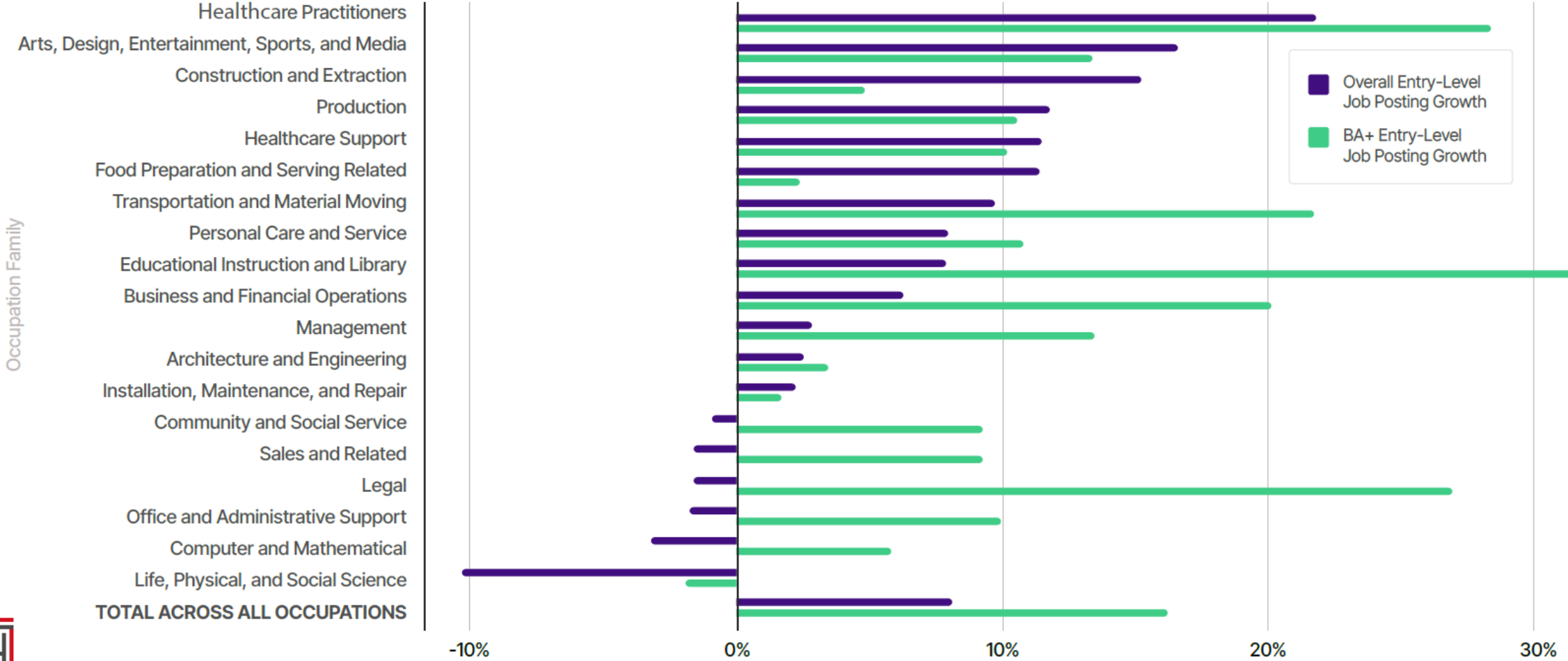
---



# Access to Entry-Level Opportunity Is Inconsistent

## Year-Over-Year Entry-Level Job Posting Growth

Source: FourOne Insights analysis of job postings data from Lightcast.

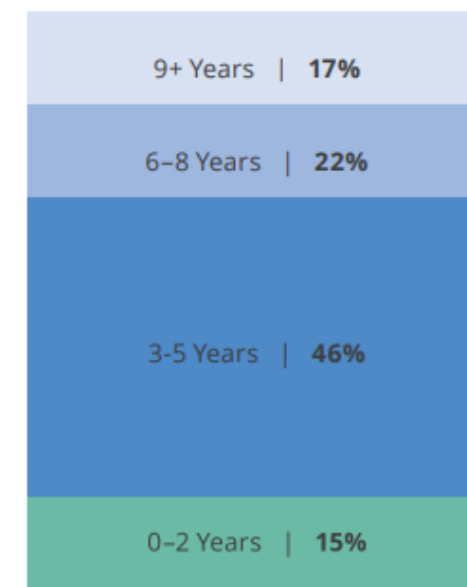
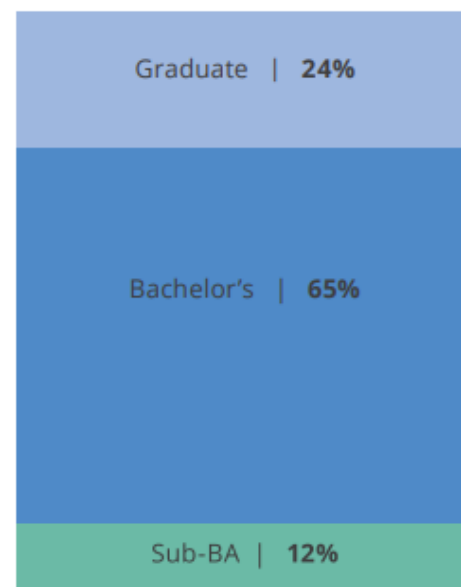


# The Cybersecurity Career Ladder is Missing a Rung

Employers request heightened education and experience levels, preventing new workers from entering the field

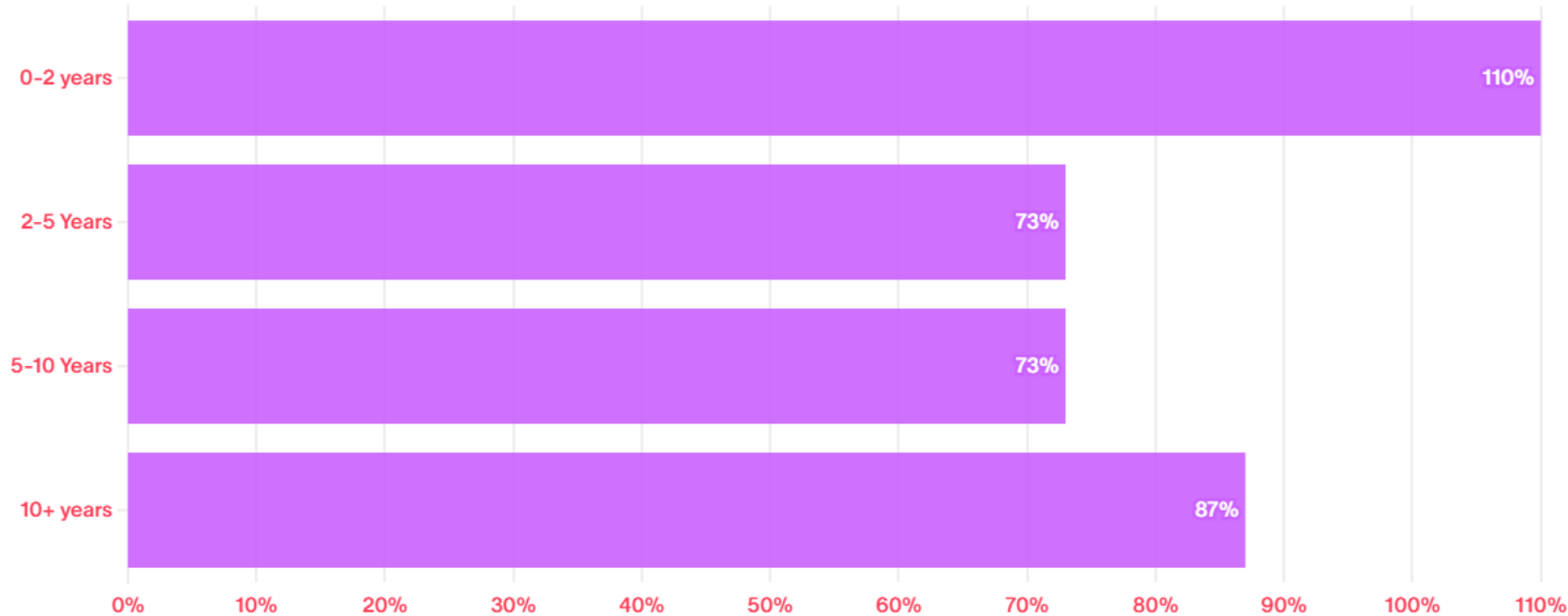
Cybersecurity education requirements

Cybersecurity experience requirements



# We Need More Cyber Workers, But The Talent Pipeline is Clogged

Cybersecurity Supply and Demand Ratio by Experience Level



We don't have enough entry points to cybersecurity, creating a dearth of experienced talent

Note: Experience levels are categorized into different ranges denoting the number of years of experience. Each range is defined by a lower limits (inclusive) and an upper limit (exclusive). Date range: September 2023-August 2024

Source: Lightcast



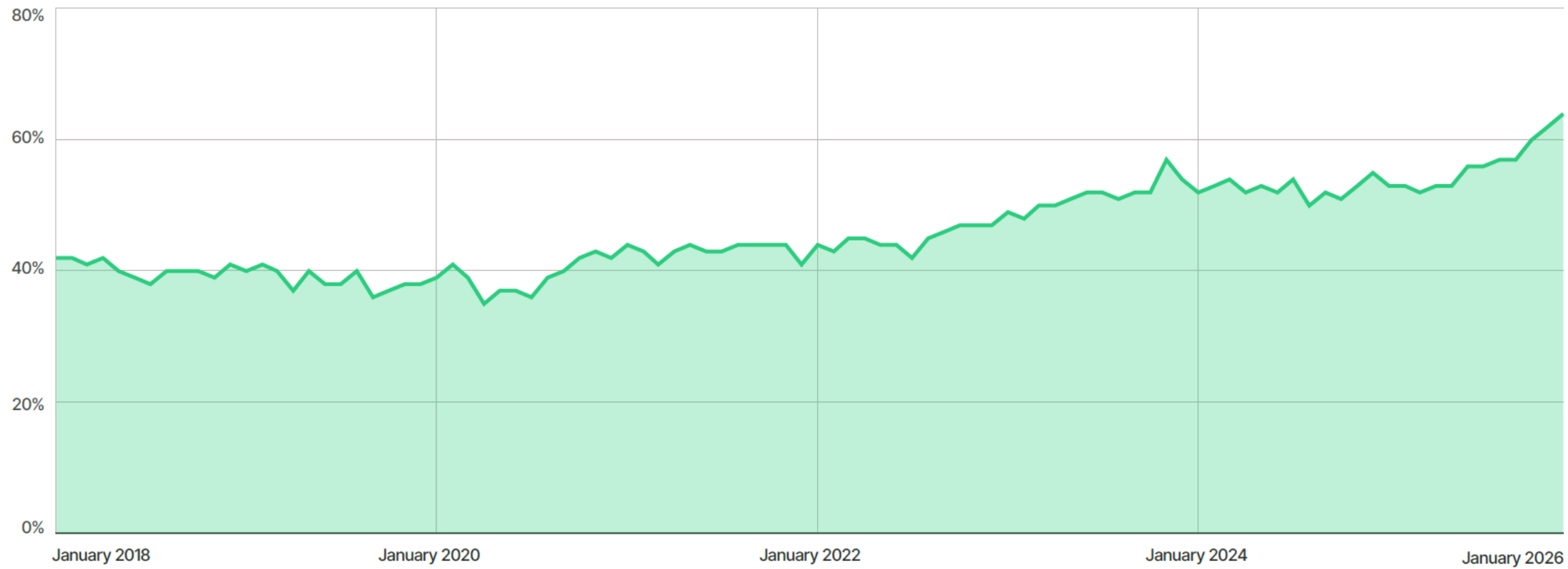
# The AI Turning Point

Will Hype Transform into  
Operational Maturity?



# AI Adoption is Spreading Across Organizations

Share of AI Job Postings Outside of Tech Jobs

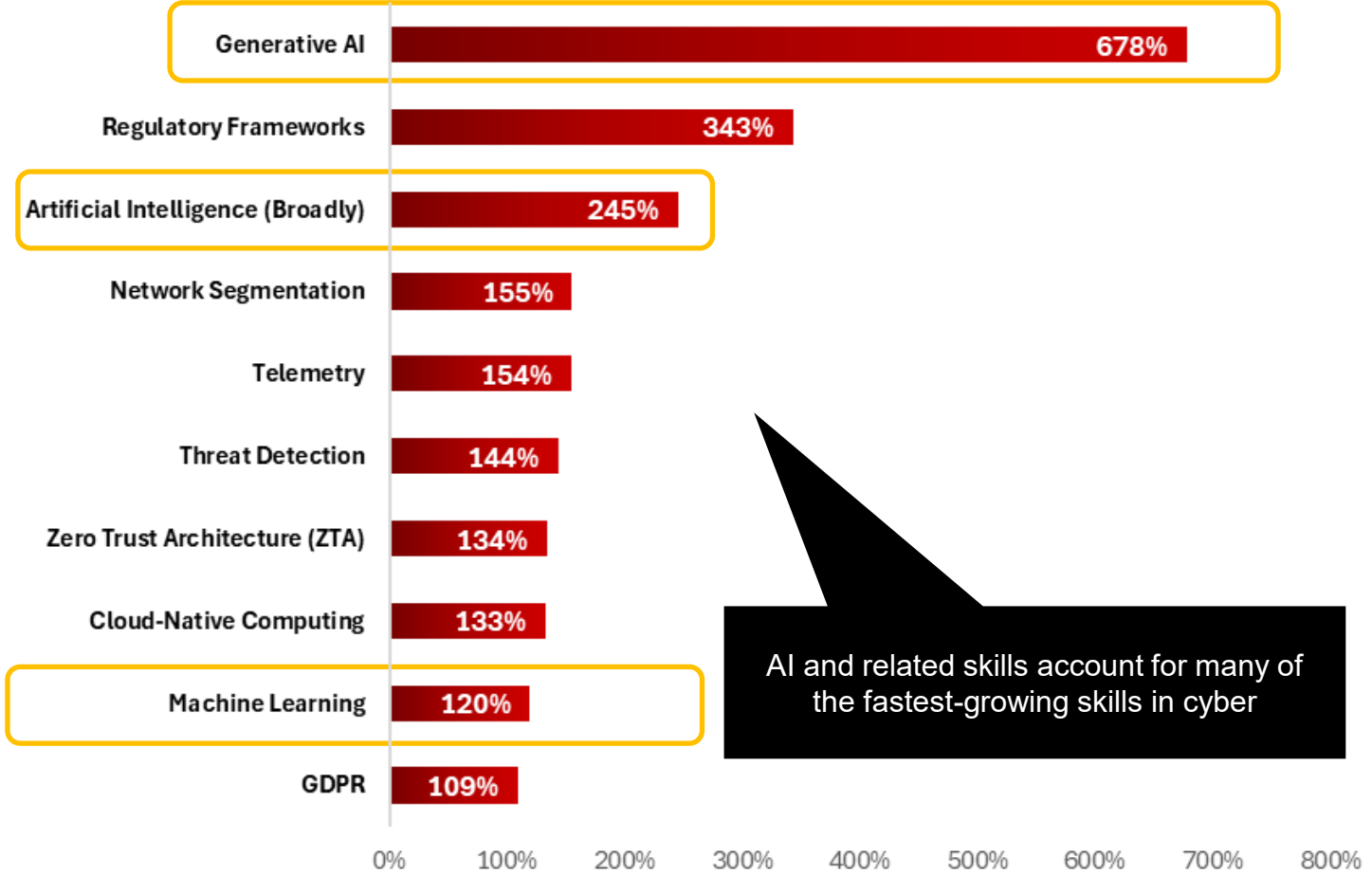


# AI is Driving Skill Evolution in Cybersecurity

Since 2023,  
**23%**

of key cybersecurity skill requirements have changed

Fastest-Growing Skills in Cybersecurity  
2023 to Oct. 24 – Sep. 24



AI and related skills account for many of the fastest-growing skills in cyber



# Generative AI is Reshaping Cyber Workflows

## Highest-Value Tasks GenAI is Automating or Augmenting: Infosec Analysts

**Estimated Share of Work Automated or Augmented by GenAI: Infosec Analysts**

**17% - 26%**

Task	Estimated Annual Cost Per Task Without AI	Frequency of Task Automated with GenAI	Frequency of Task Augmented with GenAI
Modify computer security files to incorporate new software, correct errors, or change individual access status.	\$15,657	64%	0%
Develop plans to safeguard computer files against accidental or unauthorized modification, destruction, or disclosure and to meet emergency data processing needs.	\$14,104	0%	42%
Perform risk assessments and execute tests of data processing system to ensure functioning of data processing activities and security measures.	\$7,351	71%	22%
Coordinate implementation of computer system plan with establishment personnel and outside vendors.	\$4,661	68%	23%
Document computer security and emergency measures policies, procedures, and tests.	\$4,123	51%	36%



# The Top-Heavy Organization

Will Managers Drown in  
Added Responsibility?



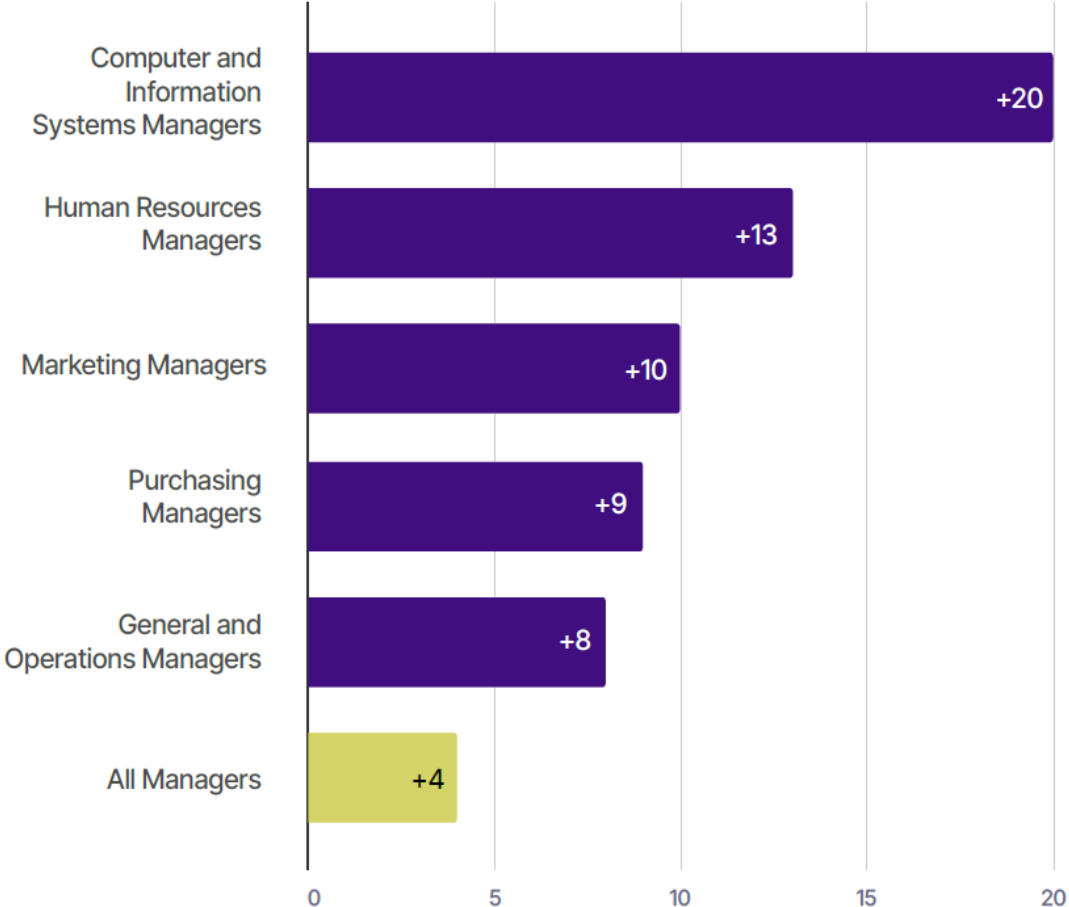
# Responsibilities are Piling Up for Managers

From 2022 – 2024, managerial employment grew by

# 1.1 Million

This was the largest absolute increase of any job family

### Growth in the Number of Commonly Requested Skills: 2022 - 2025



# Skills in Managerial Cyber Roles Are Changing Rapidly

Role	Share of Key Skills that are Growing Rapidly	Key Fast-Growing Skills Since 2023
Cyber Architect	63%	Artificial Intelligence (+221%) GDPR (+187%) Google Cloud Platform (+163%)
CISO	60%	Third Party Risk Management (+768%) Scalability (+483%) Artificial Intelligence (+348%)
Cyber Manager	60%	Artificial Intelligence (+209%) Google Cloud Platform (+174%) Continuous Improvement Process (+153%)
Cyber Product Manager	56%	Service Offerings (+1,100%) Artificial Intelligence (+477%) Cyber Threat Intelligence (+315%)
Penetration Tester	49%	Artificial Intelligence (+279%) ISO/IEC 27001 (+158%) MITE ATT&CK Framework (+92%)
Cyber Engineer	45%	Threat Detection (+152%) GDPR (125%) Cyber Threat Hunting (+94%)
SOC Analyst	30%	ISO/IEC 27001 (+256%) Microsoft Sentinel (+248%) Continuous Improvement Process (+169%)
Cyber Analyst	5%	Cyber Threat Hunting (+65%) Windows PowerShell (+35%) Cyber Threat Intelligence (+21%)

CISOs and Cyber Managers see their skill requirements shifting faster than almost any other role



Cybersecurity  
Managers  
**Need Future-  
Proofing**

**78%**

Share of cybersecurity managers with no prior  
managerial experience

**11 Years**

Average length of time since cybersecurity  
managers graduated with their most recent degree



# The Talent ROI Reckoning

Will Organizations Learn to  
Maximize Talent Investments  
with Strategic Planning?

---

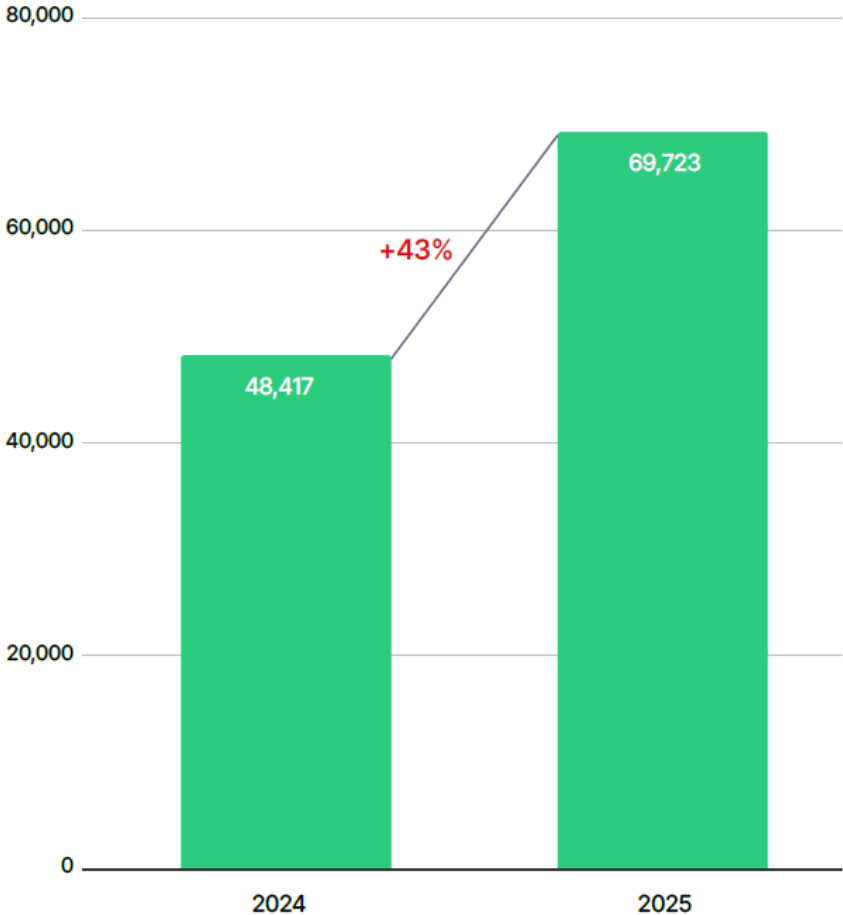


# Employers are Prioritizing Strategic Workforce Planning

In 2025, employer demand for skills related to workforce planning and talent strategy jumped

**43% YoY**

Job Openings Requesting workforce Planning or Talent Strategy Skills



# Cyber Employers Can Boost Talent ROI by Training for High-Growth, High-Value, Undersupplied Skills

Fastest-Growing Cyber Skills

Skill	Growth since 2023	Available Workers Per Opening (Aug. 25)	Salary Premium
Generative AI	678%	0.8	\$32,640
Regulatory Frameworks	343%	0.1	\$10,880
Artificial Intelligence (Broadly)	245%	0.3	\$28,544
Network Segmentation	155%	0.2	\$6,016
Telemetry	154%	0.1	\$10,880
Threat Detection	144%	0.3	\$4,992
Zero Trust Architecture (ZTA)	134%	0.1	\$15,232
Cloud-Native Computing	133%	0.1	\$13,952
Machine Learning	120%	0.4	\$29,568
GDPR	109%	0.3	\$7,040
All Cyber Jobs	8%	1.0	NA

Many emerging cybersecurity skills boost salaries by \$10k-\$20k+



# Cyber Employers can Improve Hiring Outcomes by Rightsizing Job Requirements

## Sample Cybersecurity Job Requirements

### IT Security Analyst

#### Qualifications

- ~~2+ years of progressively increasing responsibility in the areas of~~ information security, cloud security, or cybersecurity
- Bachelor's degree in IT, cybersecurity or related area of study,
- ~~Prior cloud (AWS) experience~~
- Strong understanding of ~~restful API development, SDLC processes, and security automation desired~~
- Experience with multiple ~~environments and operating systems, devices and databases including Windows Server, Active Directory, VMWare, Azure, AWS.~~
- Strong analytical and problem solving skills
- Strong Incident Response background is preferred
- Fundamental understanding of security related technologies such as SIEM and SOAR
- Must have/obtain and maintain one or more Cloud or Security certifications such as AWS, Azure, CISSP, CISA, CISM, CIPT, SSCP, CCSP
- Strong understanding of information security standards, concepts, controls, testing ~~techniques and technical risk assessment~~

Removing a BA requirement  
**Saves \$16,000 and grows entry-level candidate pool by 61%**

Building, not buying, emerging cybersecurity skills  
**Saves \$10,000+ for each emerging skill**

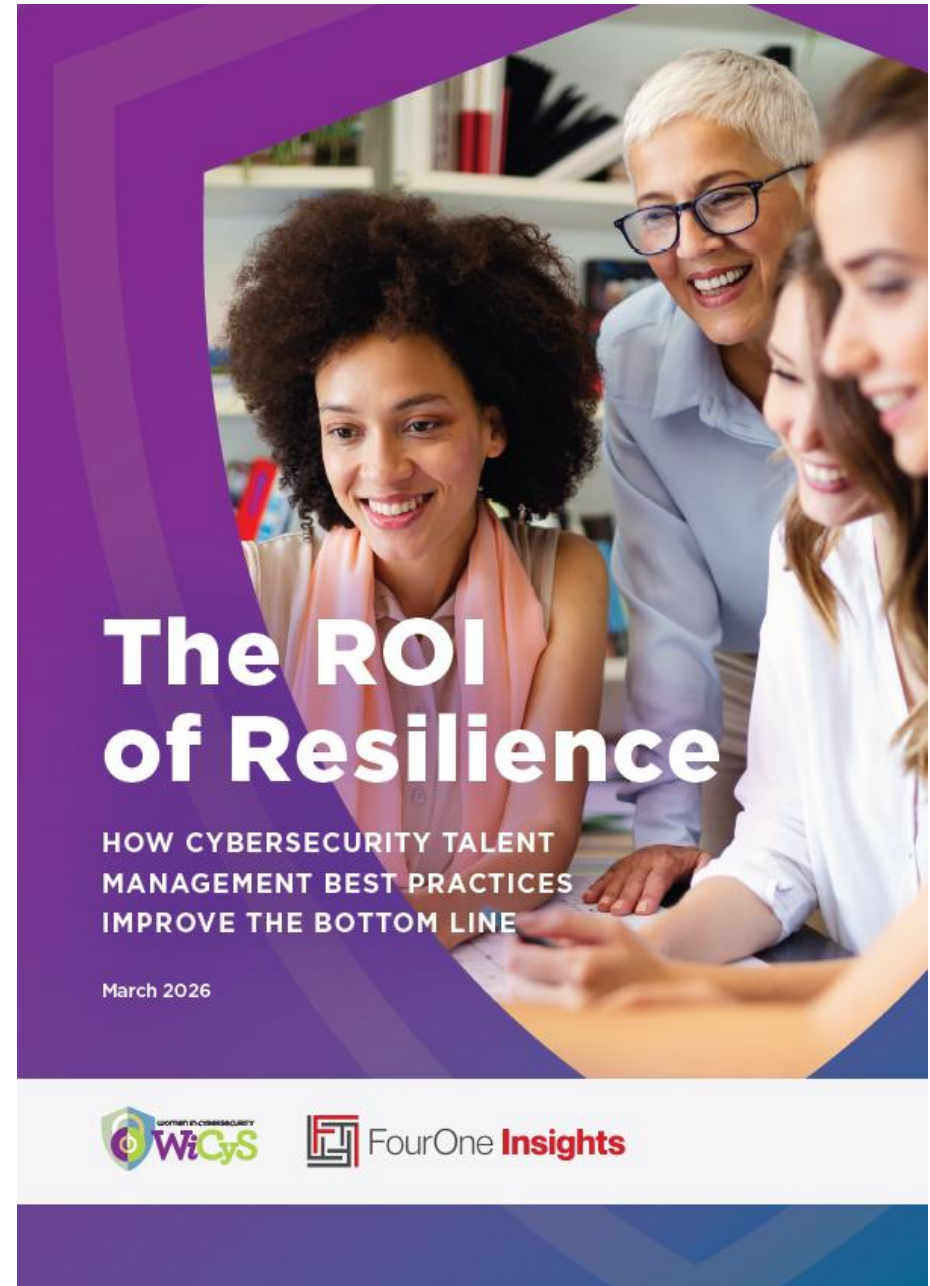
Eliminating specific certification requirements  
**Drops average salary costs by \$9,000**



# How Can Employers **Boost Cyber Talent Resilience and ROI?**



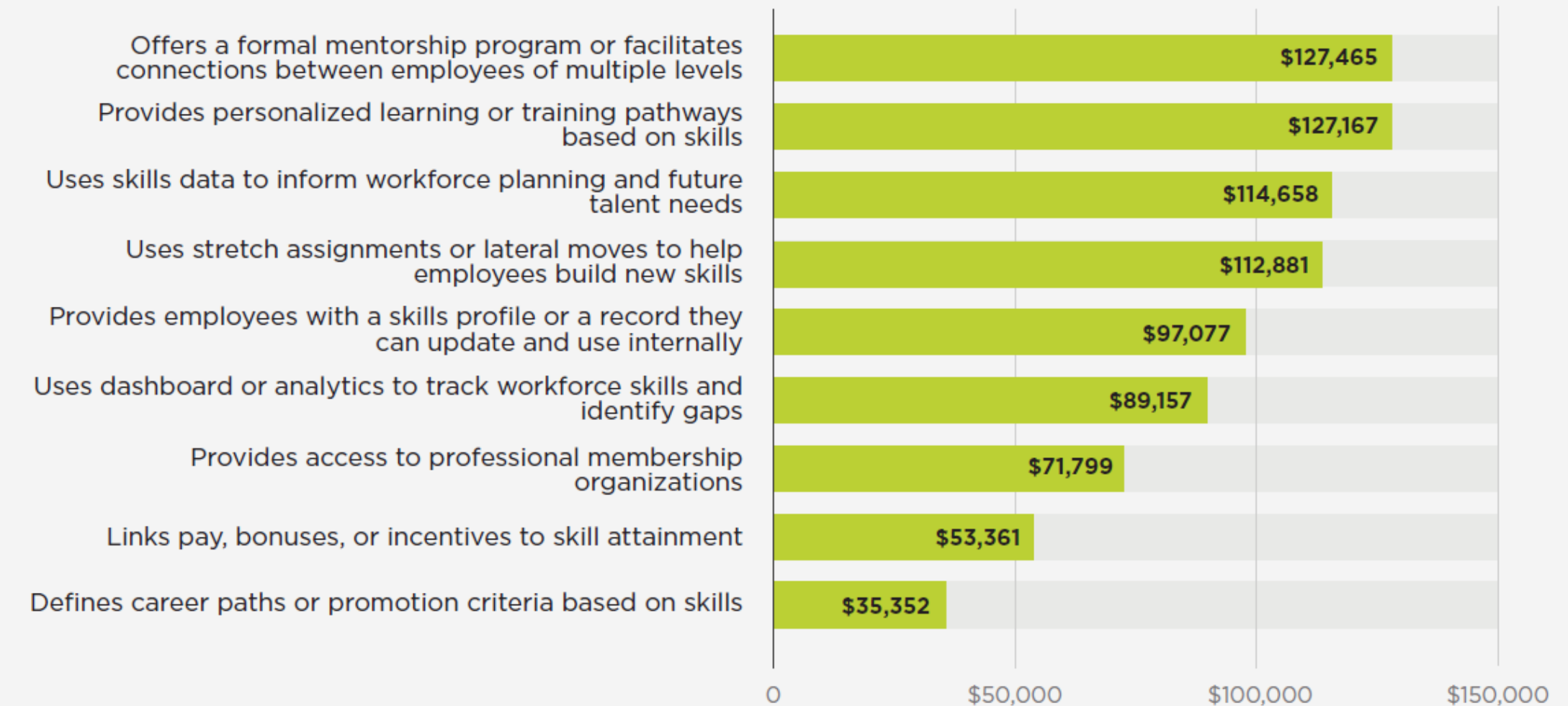
# Quantifying the ROI of Cyber Talent Resilience



# Skills-based, Talent-friendly Practices

## Generate the Highest Returns

Average Productivity Loss Avoided Per Cybersecurity Worker by Selected Talent Practices  
(based upon average increased tenure and decreased time to fill)



# Despite the Value of These Practices, Adoption is Uneven

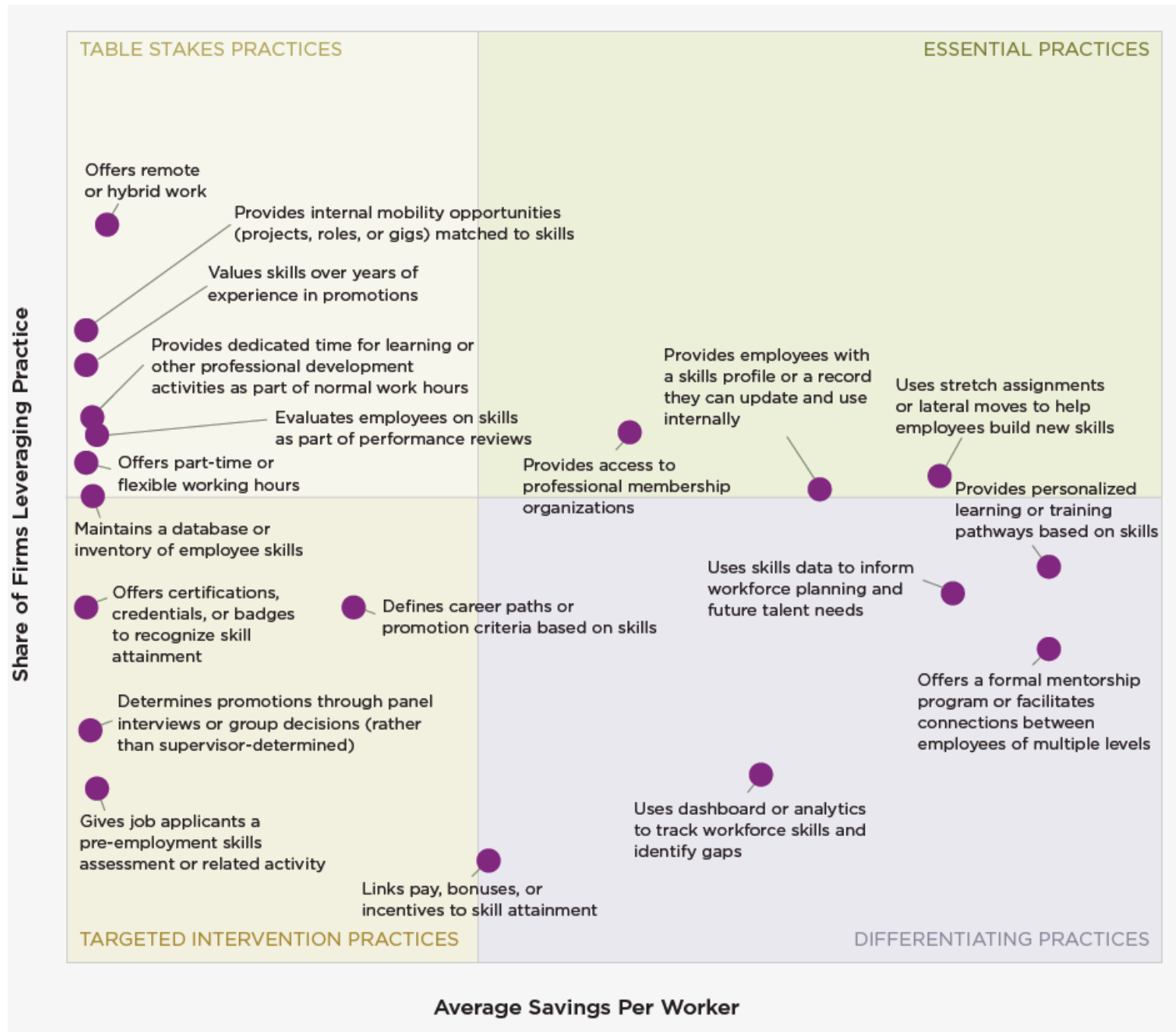
Talent Savings to Employers vs. Share of Employers Leveraging Practice

Practice	Share of Employers Leveraging Practice	Average Cost Savings Per Cybersecurity Worker
Offers a formal mentorship program or facilitates connections between employees of multiple levels	49%	\$127,465
Provides personalized learning or training pathways based on skills	55%	\$127,167
Uses skills data to inform workforce planning and future talent needs	53%	\$114,658
Uses stretch assignments or lateral moves to help employees build new skills	61%	\$112,881
Provides employees with a skills profile or a record they can update and use internally	60%	\$97,077

None of the highest-value talent practices are leveraged by more than 55% of employers



# Talent Practice Prioritization Matrix

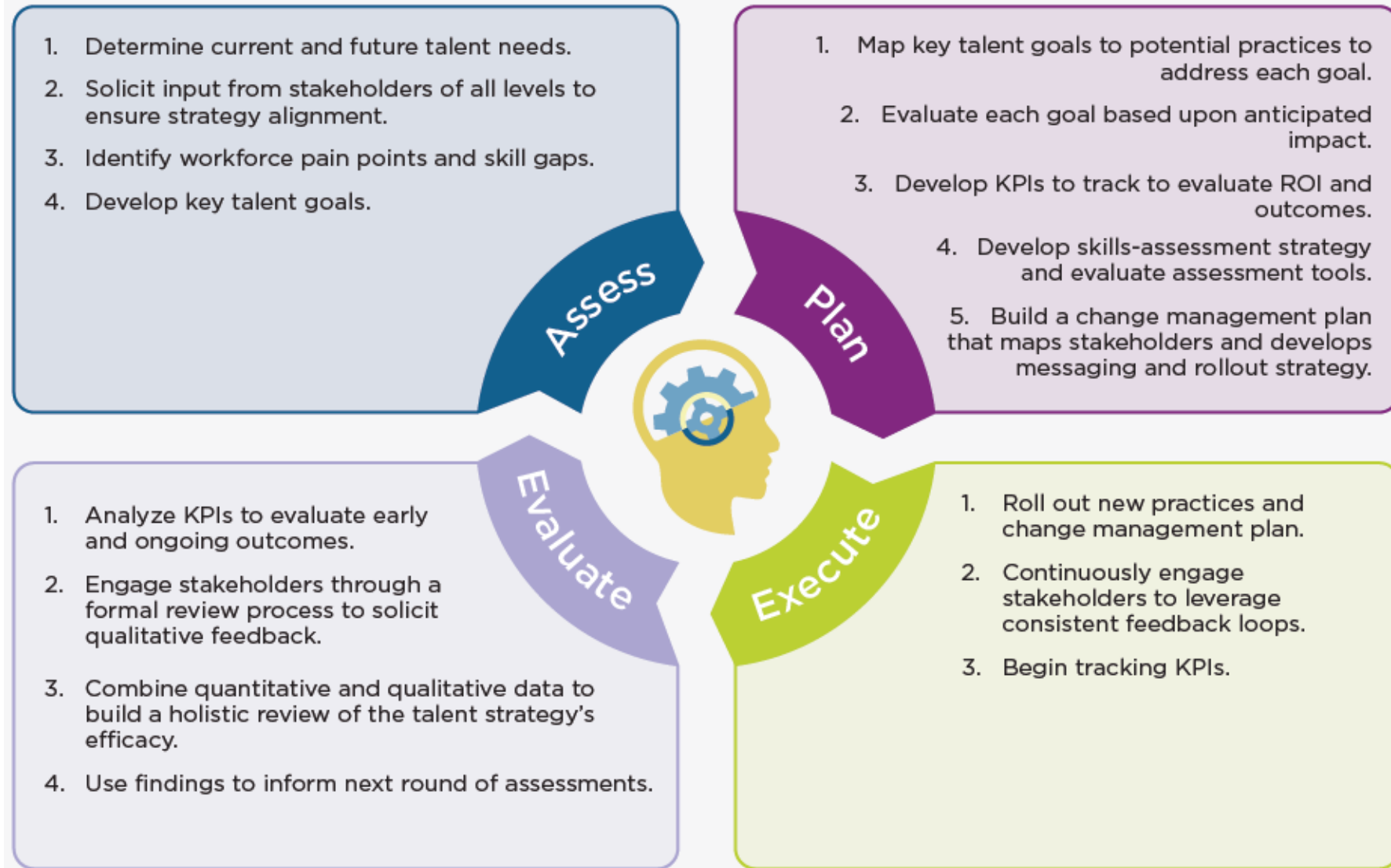


Employers Can Differentiate Their Talent Practices



# Continuously Optimize Your Talent Strategy

## Continuous Talent Optimization Framework



**Will Markow**  
Founder and CEO  
[wmarkow@fouroneinsights.com](mailto:wmarkow@fouroneinsights.com)



[info@fouroneinsights.com](mailto:info@fouroneinsights.com)



# Q&A



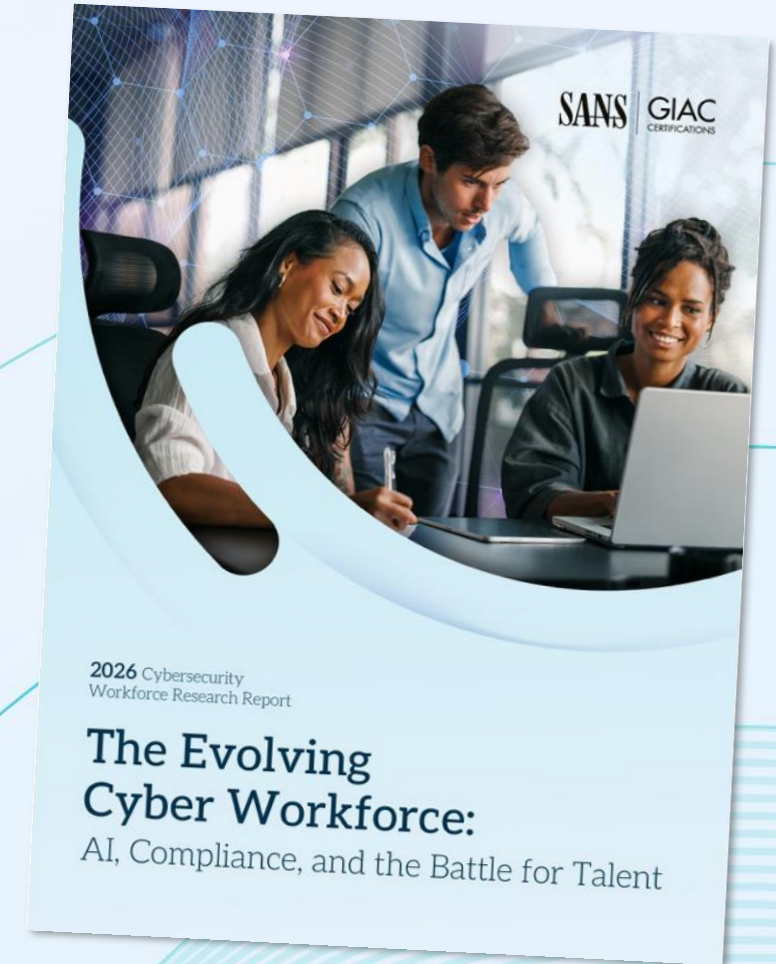
# Trends In the Cyber Workforce



Presented By:  
Brian Correia  
Director, Business Development, GIAC  
[bcorreia@sans.org](mailto:bcorreia@sans.org)

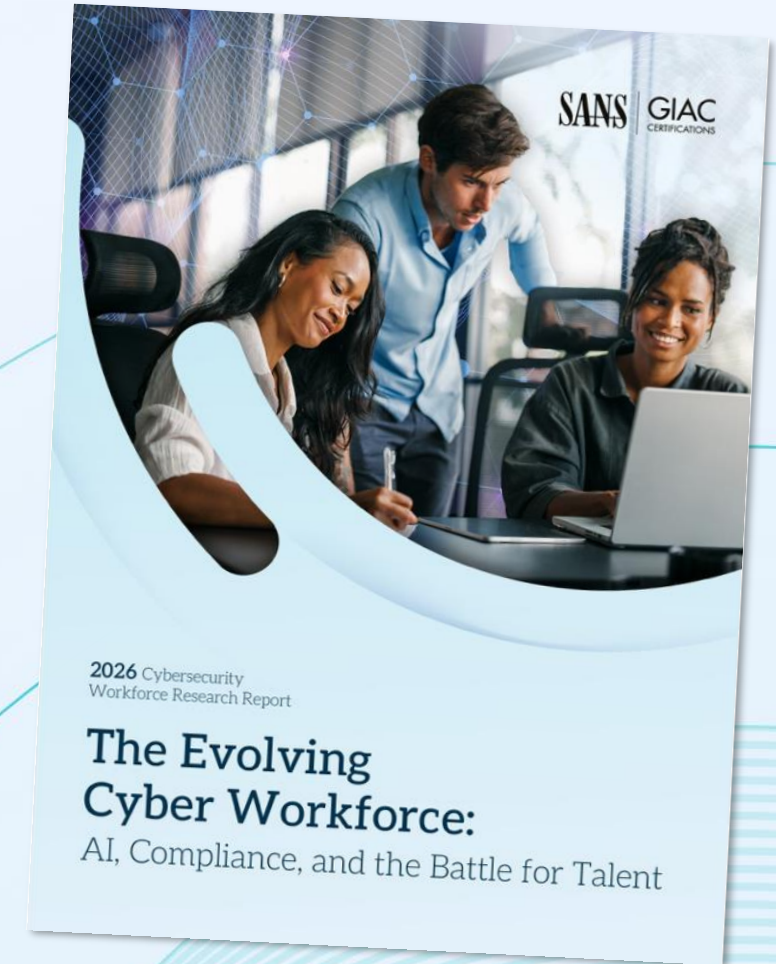
# High Level Cyber Workforce Trends

- As industry matures workforce trends:
  - AI is changing the work roles & the tasks
  - Directives are becoming more prevalent
  - Standardization of work roles/jobs
  - Larger influence throughout the organization
    - Now at C-Suite & Board Level
    - Teams such as legal/comms involved
      - Ex: Cyber Incident Reporting
  - Importance of skills validation on security teams
  - Enables the business / Not a cost center anymore



# 2026 Cyber Workforce Report

- **Goals – What does the community think**
  - Built by those who lead cyber workforce efforts
    - Cybersecurity leaders & HR Managers
    - Responsible for hiring, retention, work roles, training, and career paths
- **First Sneak Preview –**
  - **Announcement – RSAC2026 – San Francisco**
    - Monday, March 23<sup>rd</sup> @ 8:30 AM PT – Sold Out
    - Full report release to community
    - Includes workforce solutions based on trends
  - **Our third annual version**



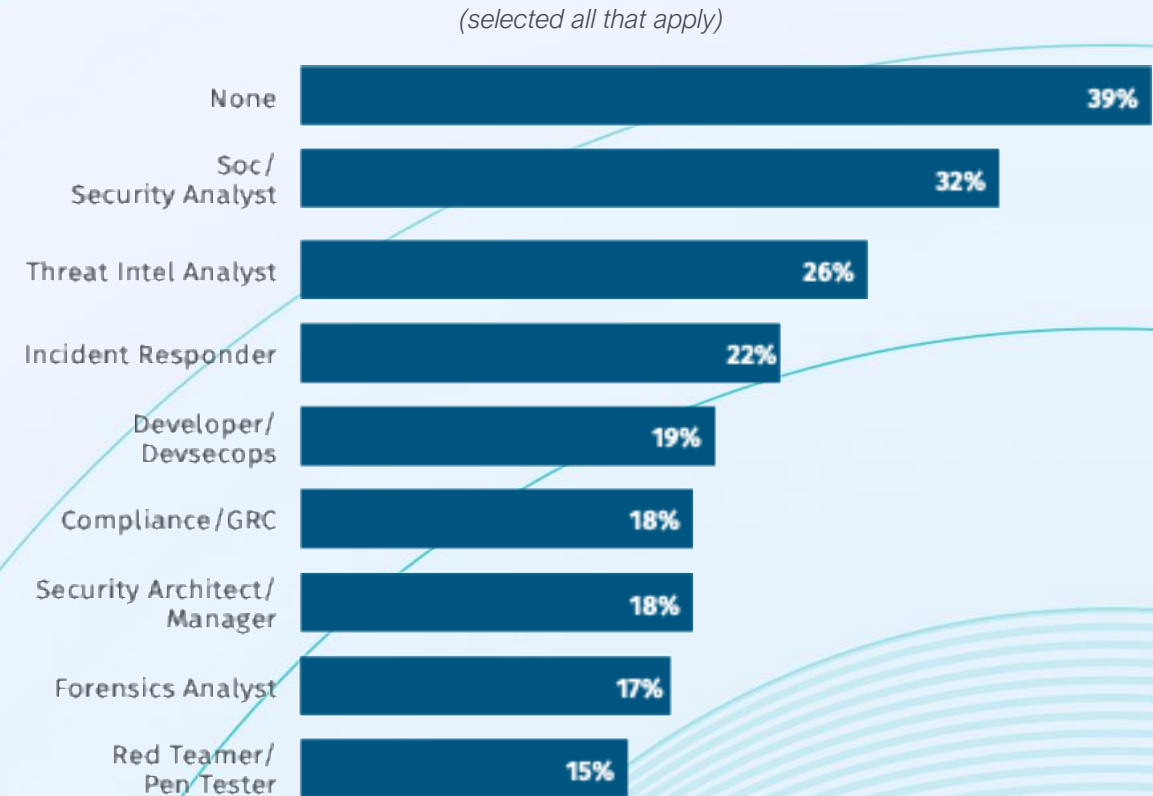
# AI's Impact on the Cyber Workforce

# Cyber Teams Already Feeling AI's Impact

## 74% of Cyber Teams are changing team size & role structures due to AI

AI is impacting entry-level jobs:

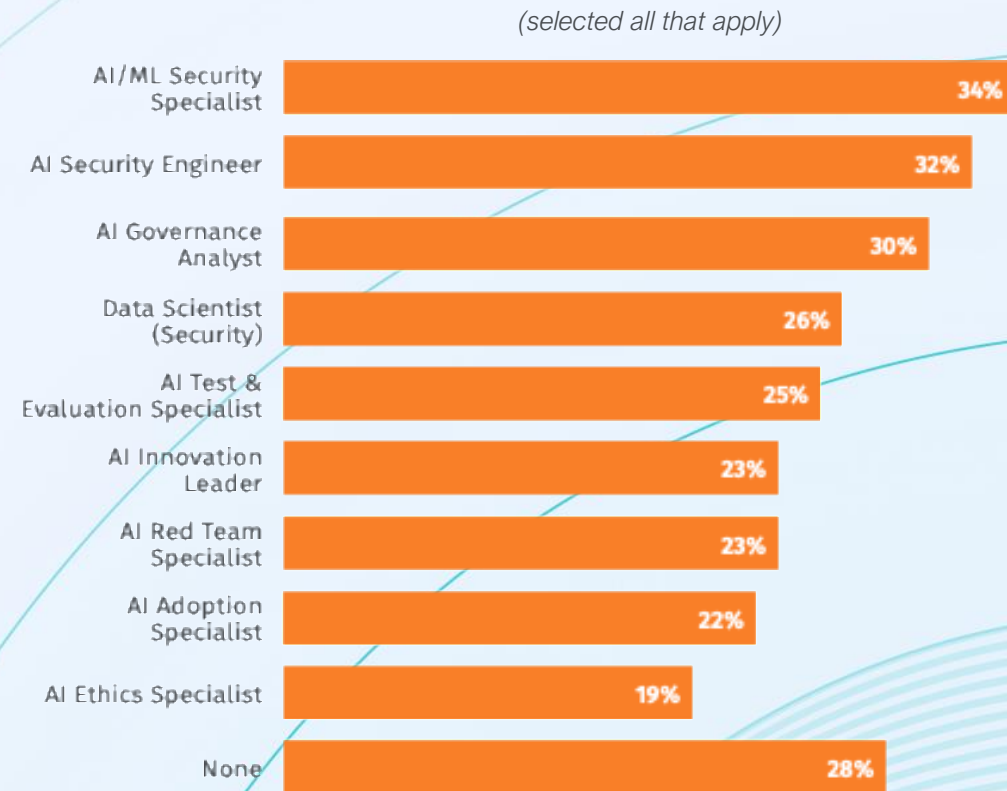
- SOC & Security Analysts leading the list at 32%
- Next are Threat Intel Analysts (26%), Incident Responders (22%), and DevSecOps (19%)
- 39% report no role reductions yet



# AI Is Creating New Roles – Still Early

AI is creating entirely new roles and specialized skills:

- 34% AI / Machine Learning Specialists
- 32% AI Security Engineers
- 30% AI Governance Analysts



# Should I be Scared AI is Going for my Job

## “No” – But Changed Landscape / Embrace Change

- Look at History
  - Invention of PC's – Productivity Doubled in 90's
  - Farming – 80% of Jobs in 1900
    - Less than 1.9% in 2000
- Bar on attacks/automation just rises equally
- Microsoft's Workforce:
  - Ex: Uses AI to automate growth pathways instead of accelerating them
- AI has limitations / bias / needs human interaction
  - Ex: SANS uses AI to map NICE Framework but SME's to finalize



# Compliance's Impact on the Cyber Workforce

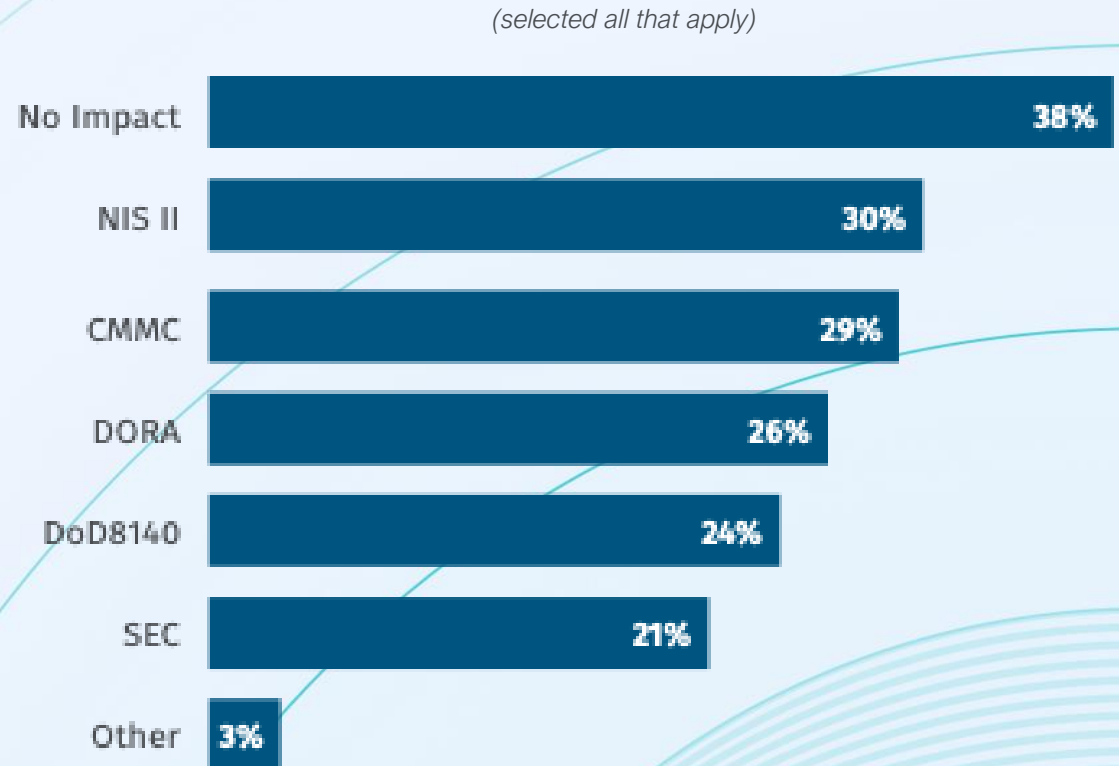
# Compliance's Impact on Hiring

## Regulatory Impact on Hiring Jumped from 40% to 95% In One Year

Chart not included on slide

Cyber operations are being reshaped:

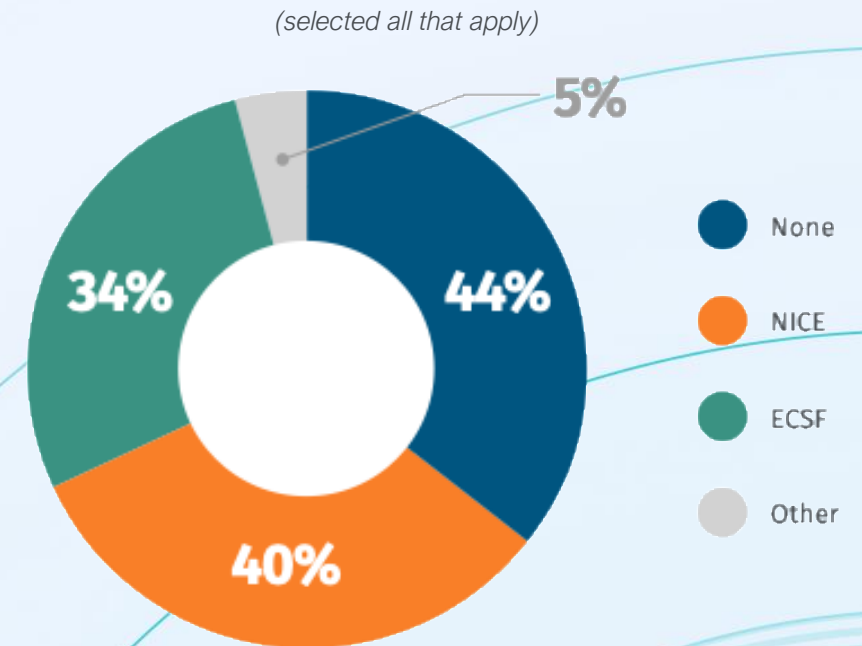
- NIS2 highest at 30% (46% in Europe)  
*Regional chart not included on slide*
- The US Military has a strong influence
  - CMMC (29% global; 38% in US)
  - DoD8140 (24% global; 32% in US)  
*Regional chart not included on slide*
- Most directives are sector or country specific



## Workforce Frameworks Define How 56% of Org's Write Job Req's

Chart not included on slide

- Last Year Was 46% - Gradual Growth
- Seeing 10% Growth Per Year
- NICE Framework standardizes roles throughout industries
  - Ex: Retail/Healthcare working together
- ECSF growth coming in from NIS2/DORA



# **Skills Impact on the Cyber Workforce**

# Skills Impact on Hiring

## 81% of Organizations are Reporting Gaps in Cybersecurity Skills

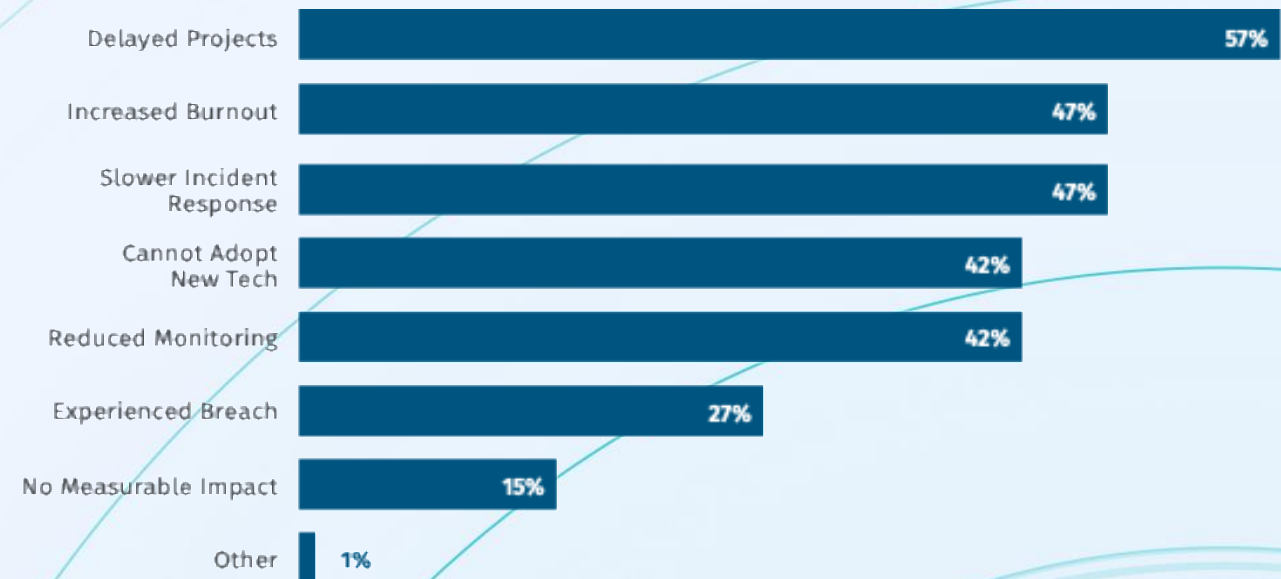
*Chart not included on slide*

- Much has been made on the “headcount problem”
- Data suggests more skills gap issue:
  - 60% skills vs. 40% headcount & growing – 52% skills last year – 20% gap

*Chart not included on slide*

- How does this affect operations:
  - 57% noted it delayed projects
  - 47% report slower incident response / Burnout
  - 42% cannot adopt new technology or maintain adequate monitoring

*(selected all that apply)*

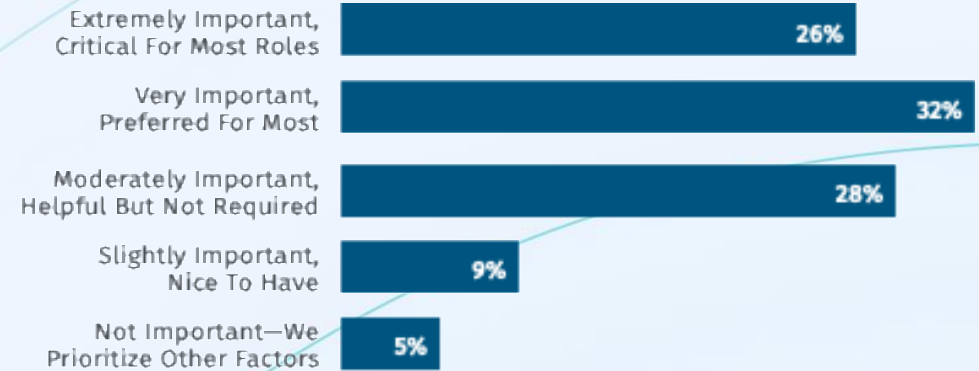


# Skills Validation

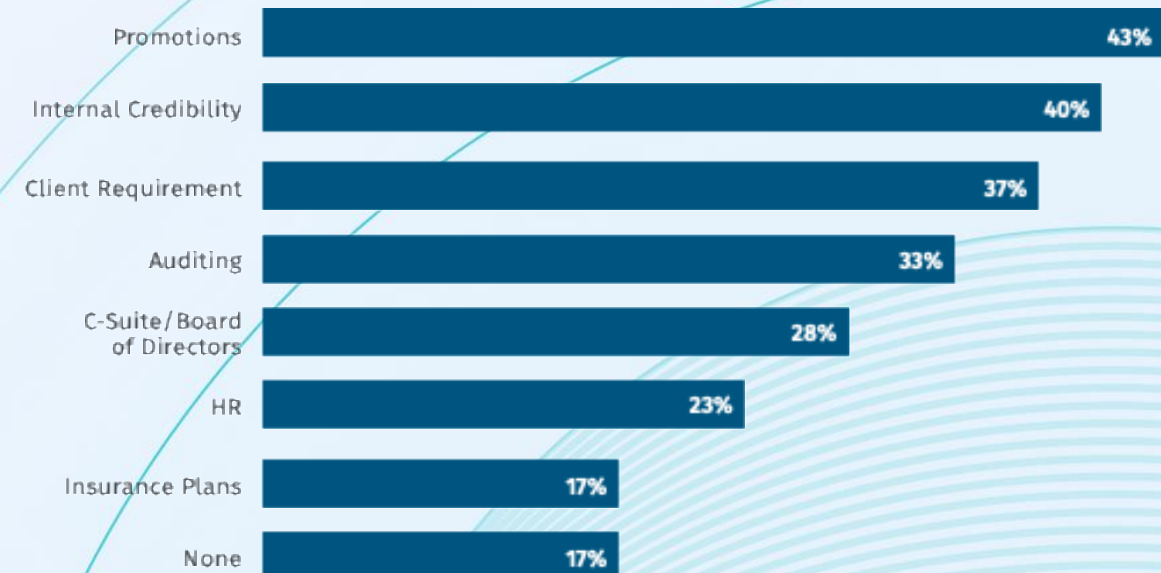
## 64% of Organizations Use Certification to Validate Skills

*Chart not included on slide*

- Only 5% view it as not important at all
- 43% use certifications for promotions
- 40% for internal credibility
- 40% for internal credibility
- External drivers
  - 37% for consulting/client requirements
  - 33% for audits
  - 28% are requested by the C-suite or board



*(selected all that apply)*



# Solutions on the Cyber Workforce Download Report

# Solutions / Download Report

## Recommended Solutions - Need to Wait till Monday, March 23<sup>rd</sup>

Today – Can sign-up to receive on kickoff day

<https://go.sans.org/2026workforce>

So much More Data (Just a Sample)

- Who Heads Up Hiring
- Challenges in Hiring and Recruiting
- Who Makes Decisions Today

Featuring Real-World Case Studies:



# Q&A



# Submit an event survey!

[https://survey.nist.gov/jfe/form/SV\\_6r3EeqAqSx6JsAm](https://survey.nist.gov/jfe/form/SV_6r3EeqAqSx6JsAm)



# NICE Webinar Series

Building Your Small Business Cybersecurity  
Team: From In-House to Outsourcing  
May 5, 2026, 2:00-3:00PM ET  
(Special Event)

Beyond Technical Skills - The Human  
Element of a Cyber Career  
May 13, 2026, 2:00-3:00PM ET



**NLST** }  **NICE**