Please Note…

This webinar and the engagement tools will be recorded.

An archive will be available on the event website.

FEDERAL CYBERSECURITY WORKFORCE WEBINAR

Providing Timely and Clear Data to Support Federal Cybersecurity Workforce Needs

FEDERAL CYBERSECURITY WORKFORCE WEBINAR

Welcome and Overview

Suzanne Nielsen
Office of the National Cyber Director

FEDERAL CYBERSECURITY WORKFORCE WEBINAR

Cyber Workforce Dashboard

Sarah Brickner
Program Analyst (Data Scientist)
U.S. Office of Personnel Management

Cyber Workforce Dashboard

- Under development – due to sensitivity of data, OPM is deliberating which data can be released to the public; no release date set
- Dummy data used for this demonstration
- EHRI-SDM data
    - EHRI-SDM data comes from Federal Agencies' Human Resource Systems
    - Onboard data (all employees at single point in time at end of FY): 3-5 months delay
    - Dynamic data (hiring and separation actions throughout FY): 6-7 months delay
- Data is presented as percentages; Visuals with 10 or less people are withheld
- Excludes data at the Department/Agency/Sub-Agency levels

FEDERAL CYBERSECURITY WORKFORCE WEBINAR

Q&A

FEDERAL CYBERSECURITY WORKFORCE WEBINAR

Track the Gap to Hack the Gap

Will Markow
Vice President of Applied Research- Talent
Lightcast

Track the Gap to Hack the Gap

Will Markow – Vice President of Applied Research

Lightcast

The Cybersecurity Talent Pipeline

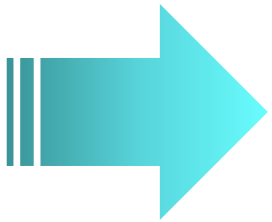
is Broken

You Can't Prepare Workers for Jobs You Know Nothing About

Overcoming Data Shortfalls to Quantify the Full Cybersecurity Ecosystem

The Problem

1. Historically, labor market information only tracked limited cybersecurity roles
2. Cybersecurity jobs evolve rapidly, but most workforce data come with a lag
3. No common language for describing cybersecurity jobs, skills, etc.



The Solution

1. Leverage real-time job posting and social profile data
2. Define cybersecurity workforce in terms of job titles, skills, and credentials required
3. Map cybersecurity jobs to NICE Framework to create common language

Tracking the Workforce of Today and Tomorrow

Lightcast Collects Workforce Data from Thousands of Sources Around the Globe

Talent Pool Estimates

Government collected data providing structured job counts to benchmark with.

Locations

Compare over 1,500 markets globally for talent supply with a singular taxonomy.

Companies

See top companies who are hiring or currently employing the talent you need.

Skills

Dig beneath vague and unreliable job titles to find the specific skills you need.

Job Postings

See real-time trends on postings in almost 750 markets around the world.

Profiles

See beyond government data to analyze over 350 million aggregated resumes to see deep insights.

Regularly featured in: the Atlantic · Forbes · Harvard Business Review · The New York Times · WSJ · USA TODAY

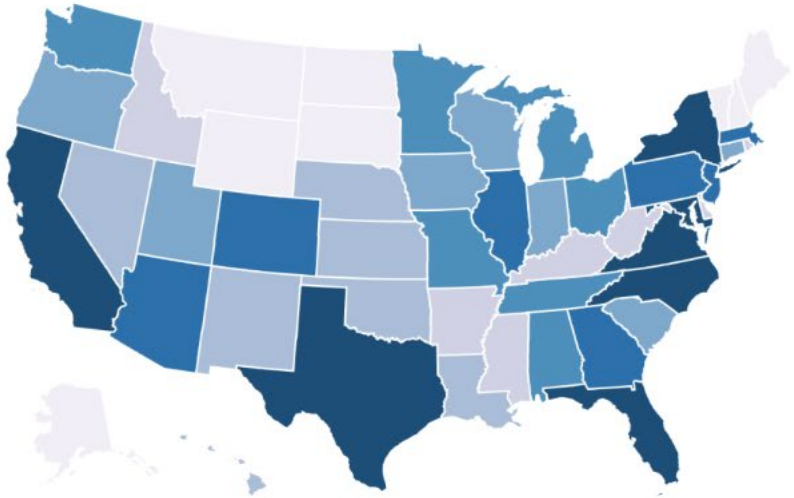
Illuminating Cybersecurity Workforce Challenges and Opportunities

Lightcast Illuminates the Public and Private Cybersecurity Job Market

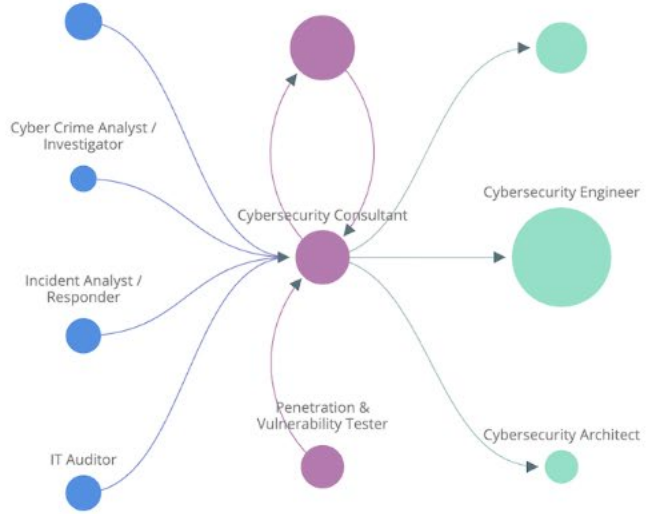
Deciphering the Cybersecurity Job Market with CyberSeek.org

CyberSeek

Interactive Map



Career Pathway



Lightcast + CompTIA + NICE NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

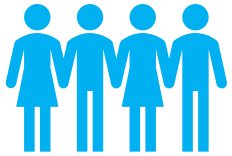
What Do the Latest Data Tell Us About the Cybersecurity Workforce?

Despite Economic Uncertainty,

Cybersecurity Job Demand Remains Strong

>

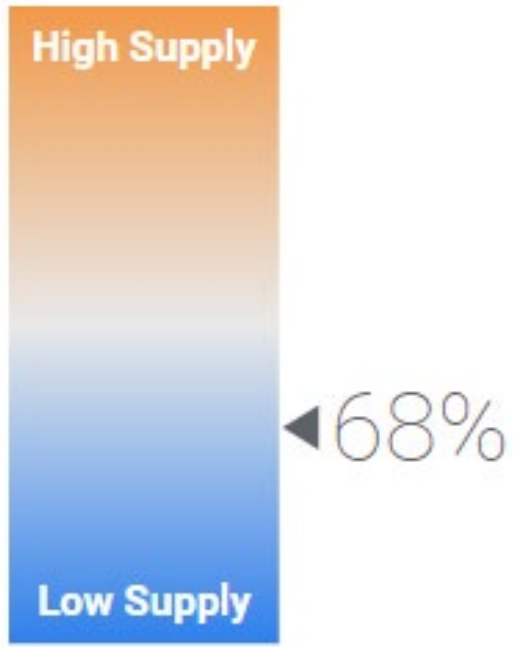
Over
755,743 cyber job openings
in the U.S. last year



Over 1.1 million
existing cybersecurity workers

But Supply
Can't Keep Up with Demand

Cybersecurity Worker Supply and Demand Ratio

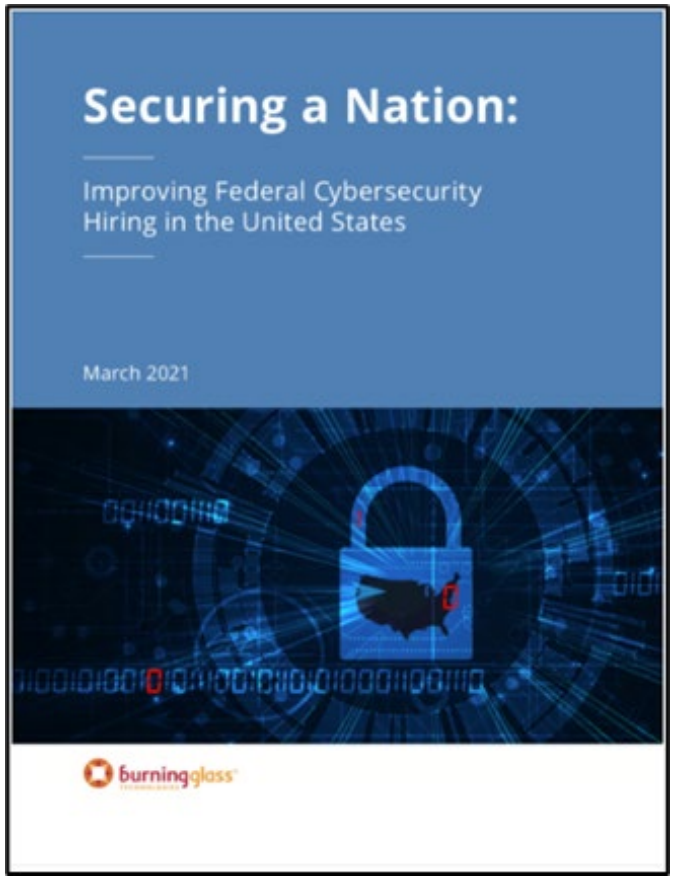


Cybersecurity jobs take
21% longer to fill
than other IT jobs

Cybersecurity jobs pay
10% higher salaries
than other IT jobs

What is Unique About Federal Cybersecurity Workforce Challenges?

Federal Cybersecurity Hiring is Fragmented

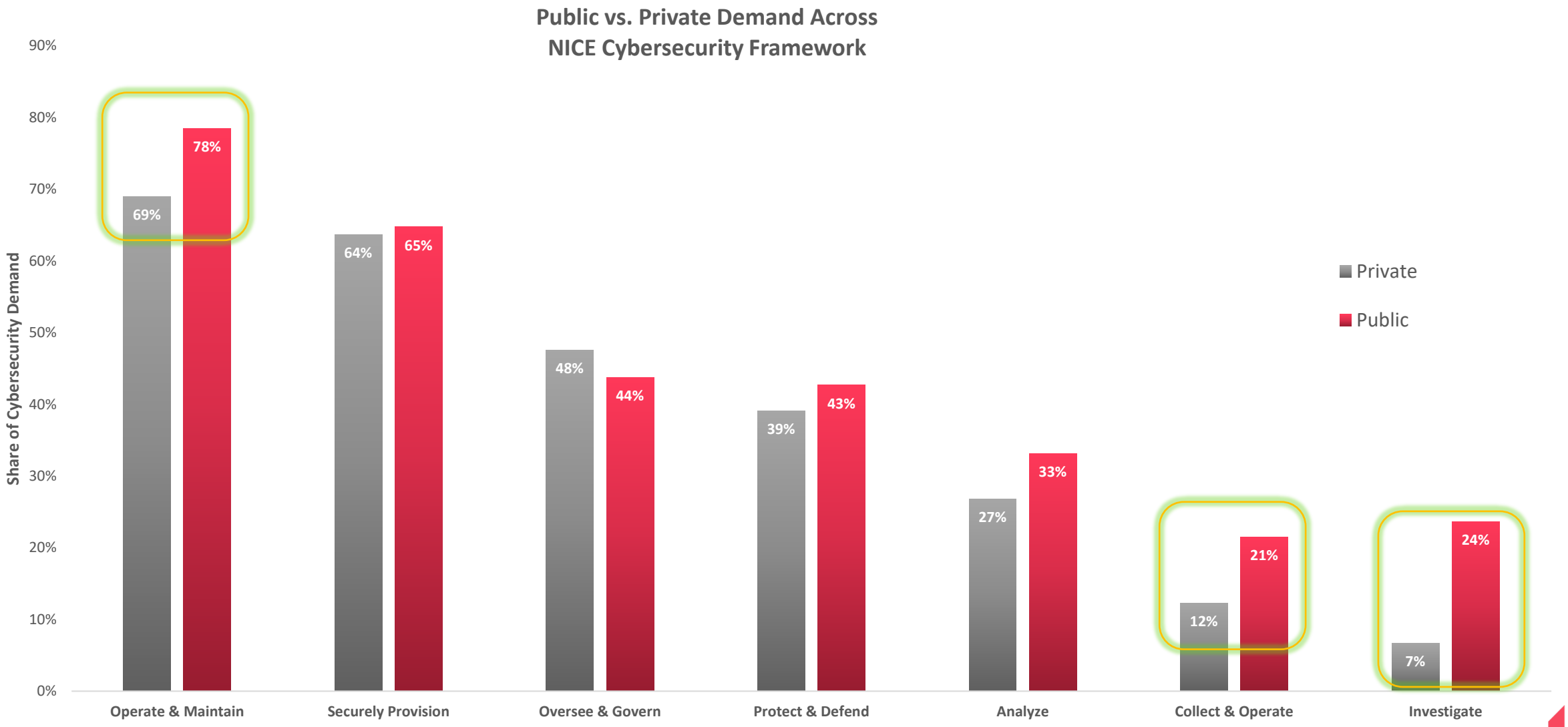


Cybersecurity jobs are posted by

165

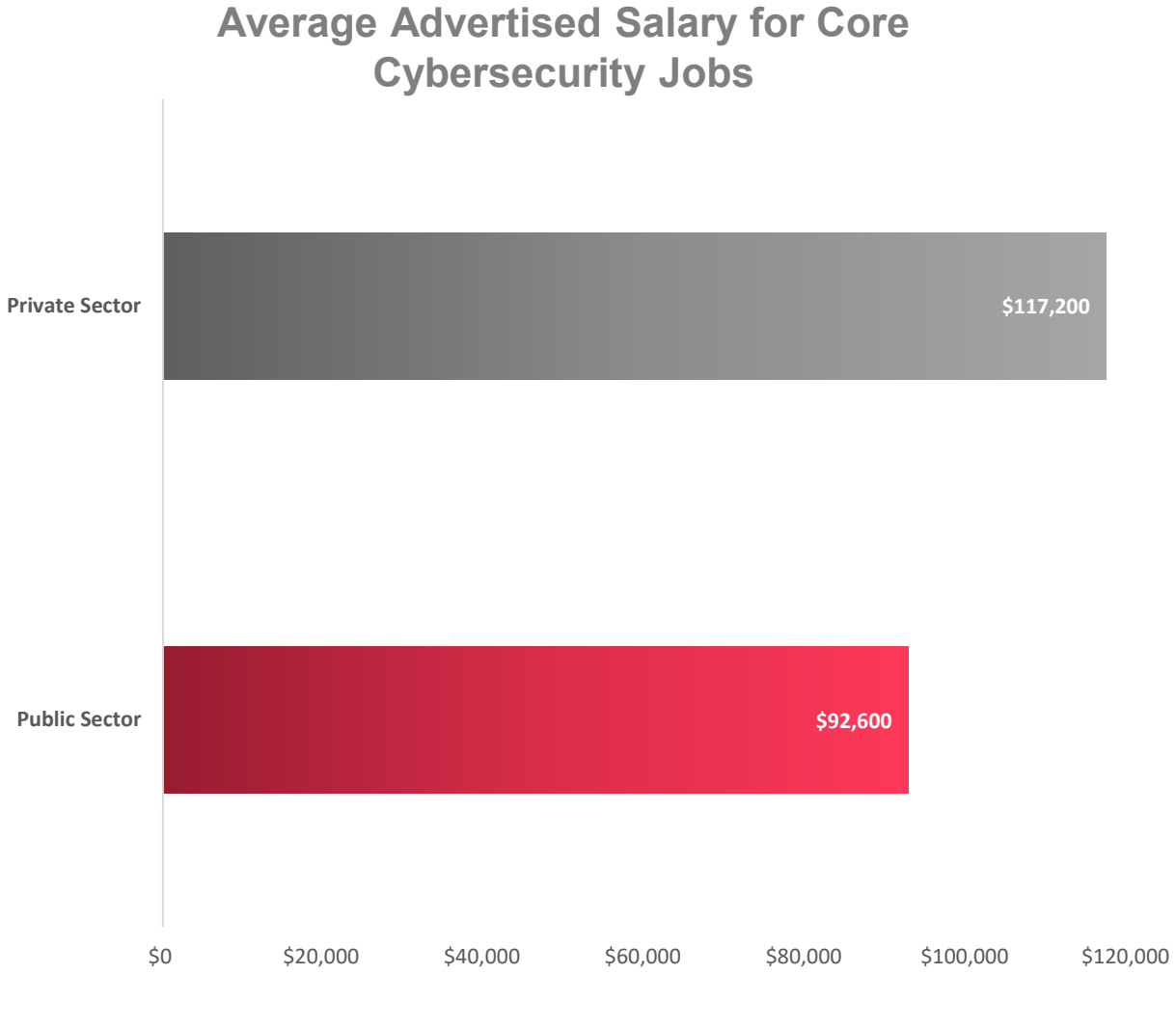
different federal entities

Public Cyber Demand is More Concentrated in Work Roles Related to Operate & Maintain, Collect & Operate, and Investigate

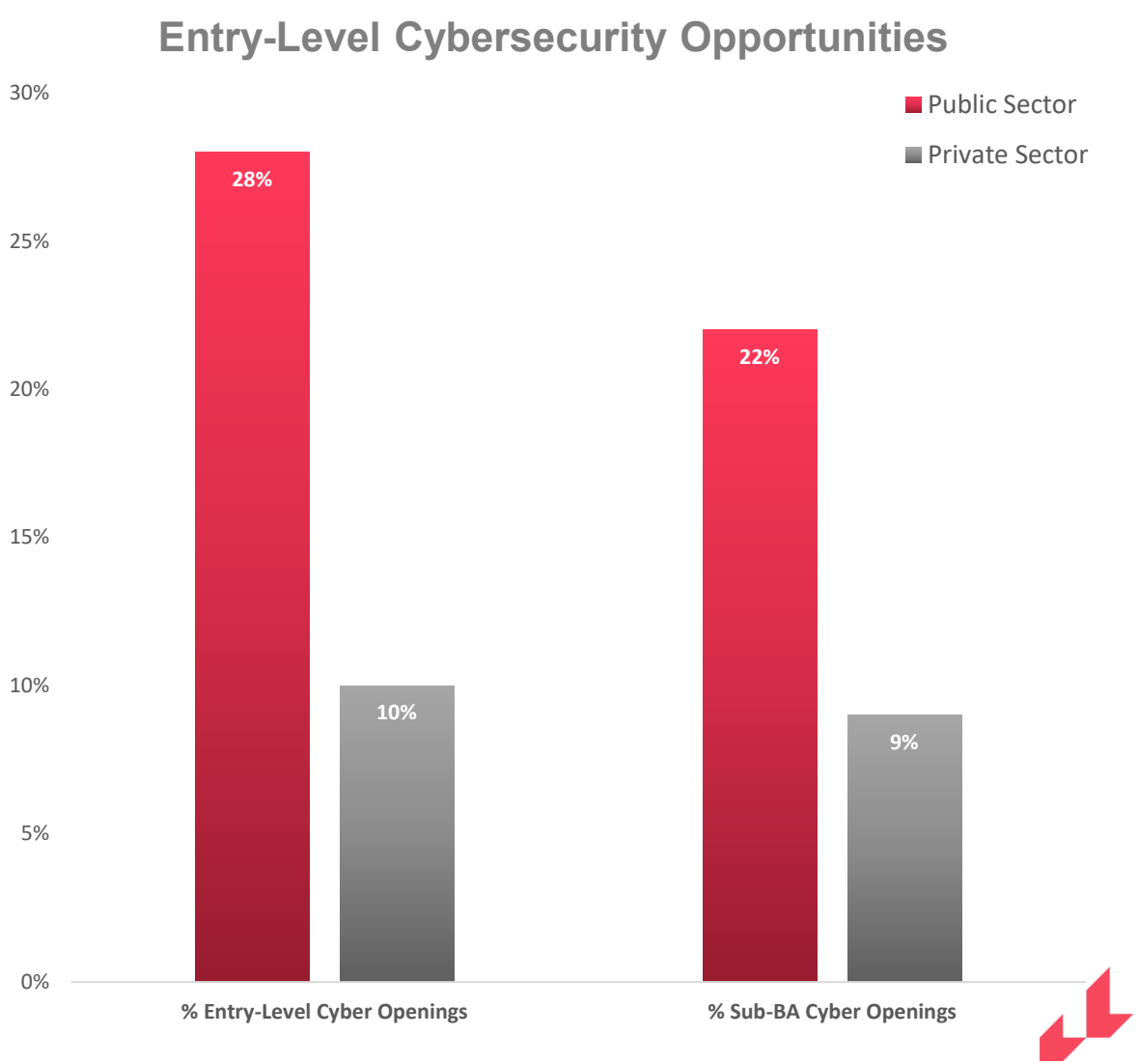


Note: One job may perform duties related multiple work roles, so the numbers will add to greater than 100%

Public Sector Cyber Jobs Struggle to Keep Up with Private Sector Pay...



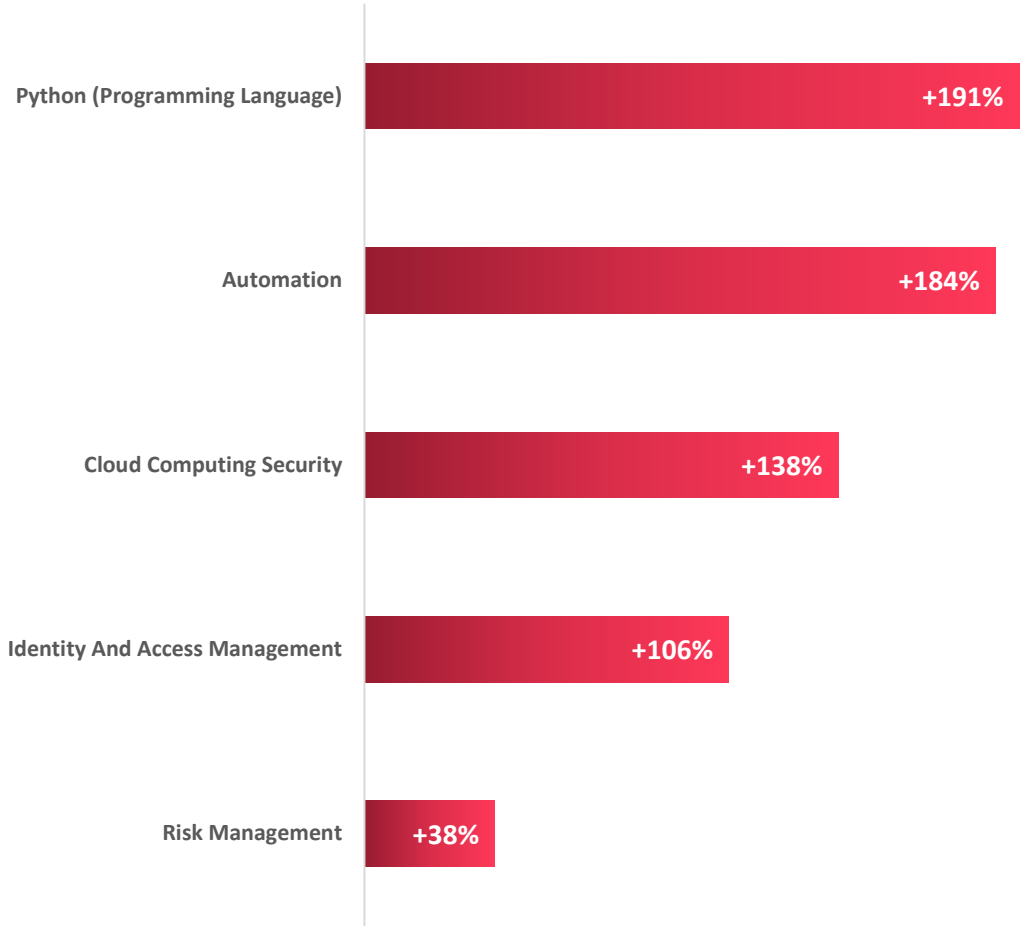
...But Offer More Entry-Level Opportunities



Private Employers Are 87% More Likely to

Emphasize Emerging High-Value Skills

Sample Cyber Skills More Commonly Requested by Private Employers Than Public Employers



Questions? Are There Other Challenges Federal Employers Face?

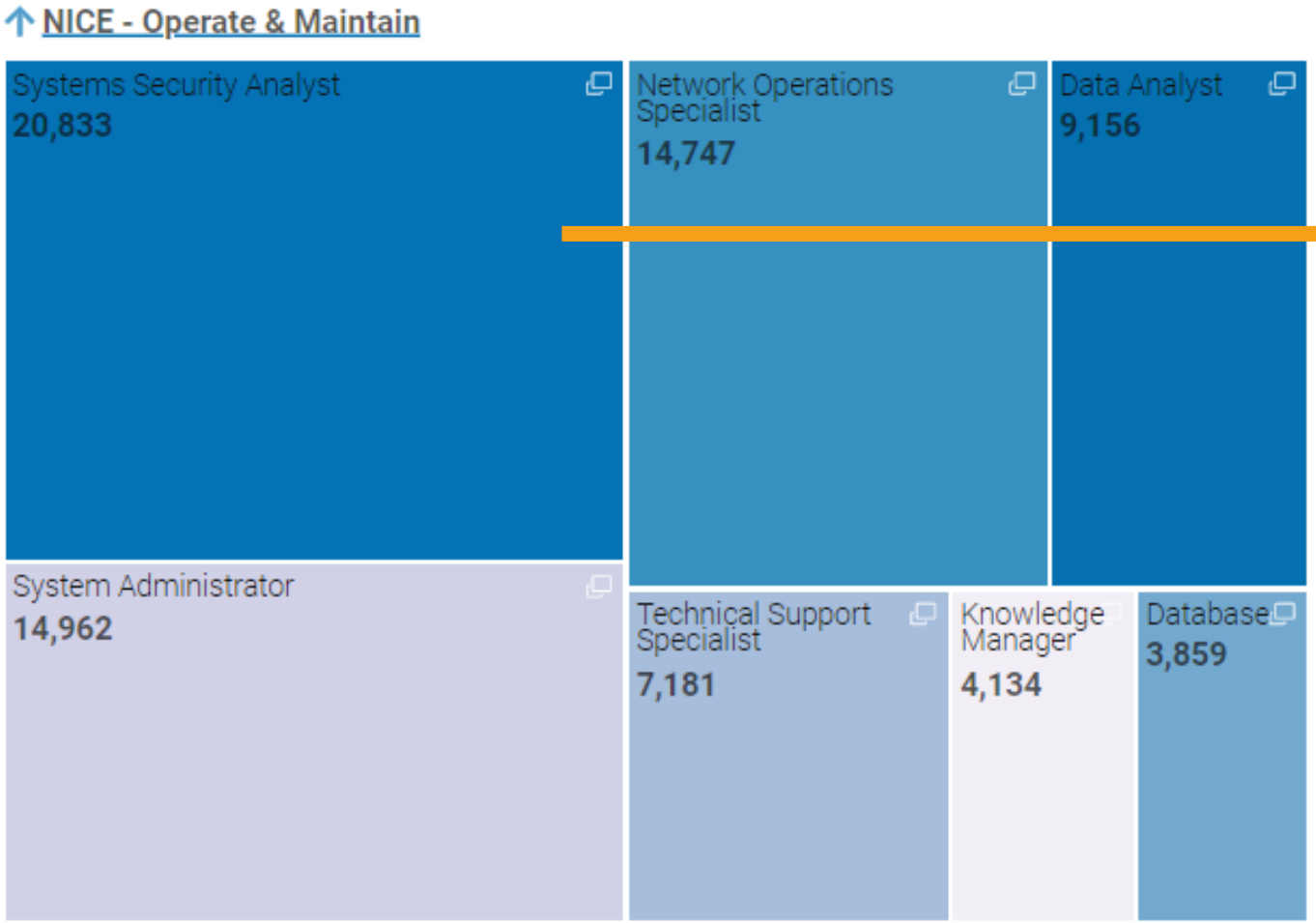
How Can the Federal Government Address its Cybersecurity Hiring Challenges?

Direct Workforce Development

Where it is Most Needed

Focus on Building the Talent Pipeline for In-Demand Work Roles

Demand by Work Role: Public Sector



Notes: The NICE Workforce Categories are not mutually exclusive- one job could perform multiple roles within the framework. The data shown here are not intended to be aggregated.

Systems Security Analyst is the most-demanded work role among public employers

Train for High-Value Skills

Arm Students with the Skills Employers Most Value…Not Just Degrees

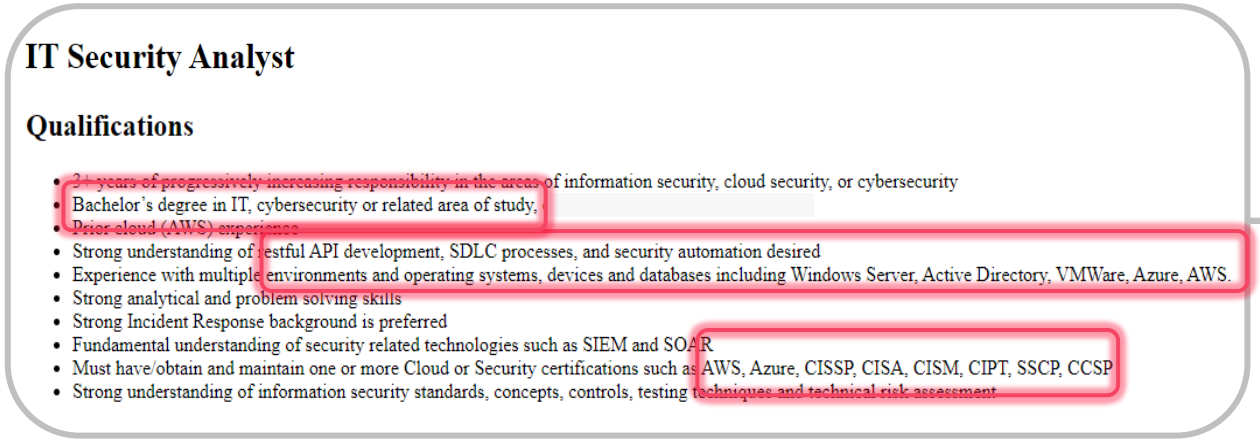
Skill	5-Year Projected Growth	Postings Oct. 2019-Sept. 202	Salary Premium
Application Development Security	164%	29,635	$12,266
Cloud Security	115%	19,477	$15,025
Risk Management	60%	57,967	$13,379
Threat Intelligence	41%	60,039	$9,609
Incident Response	37%	23,497	$5,683
Compliance and Controls	36%	54,770	$12,423
Data Privacy and Security	36%	88,527	$5,256
Access Management	32%	118,096	$6,451
Security Strategy and Governance	20%	82,952	$7,735
Health Information Security	20%	413,687	$738

Many emerging cybersecurity skills **boost salaries by $10k-$15k+**

Right-Size Job Requirements

Focus on Need-To-Haves Versus Nice-To-Haves

Sample Cybersecurity Job Requirements



IT Security Analyst

Qualifications

- 3+ 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

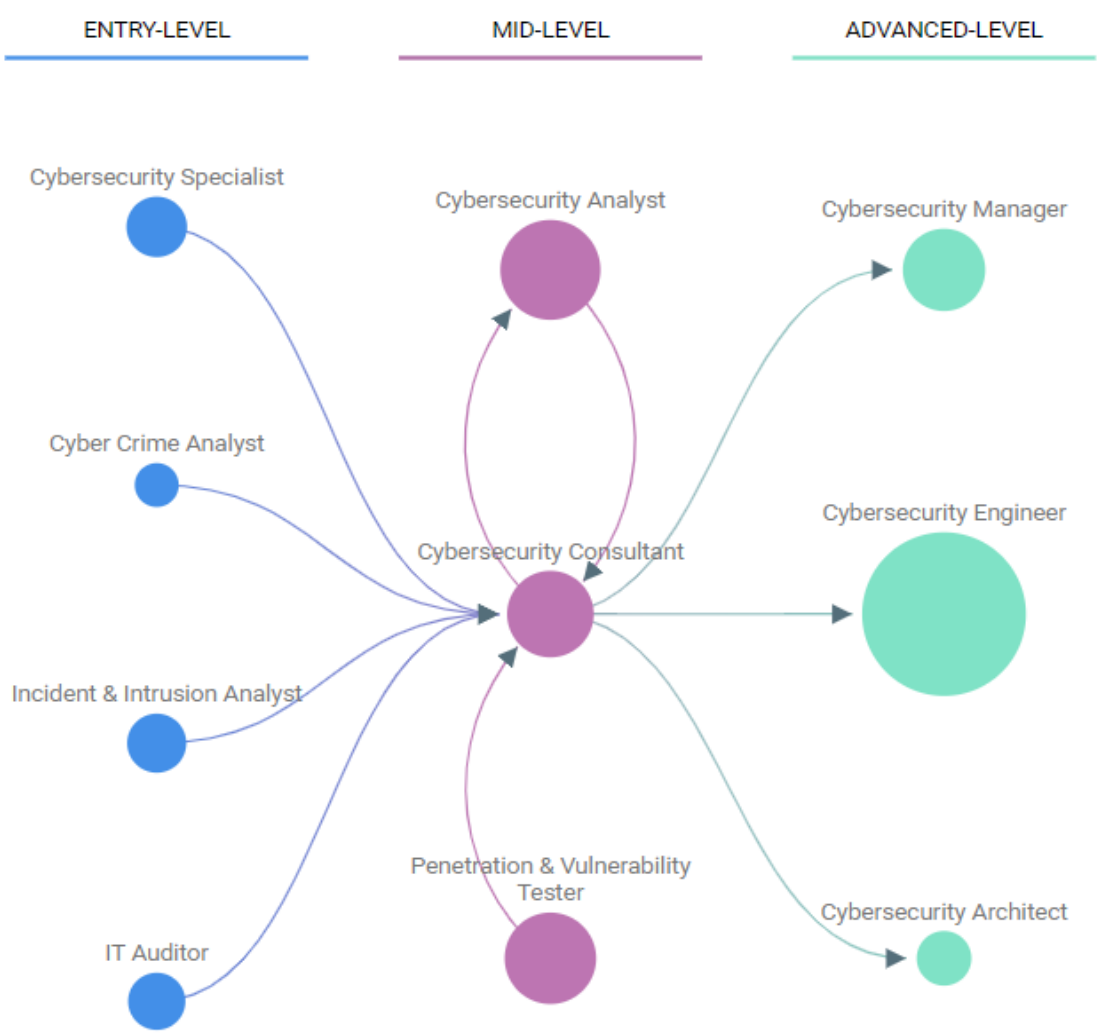
Drops average salary costs by $9,000

Unlock the Power of Pathways

Build Diverse Talent Pipelines with Cybersecurity Career Pathways

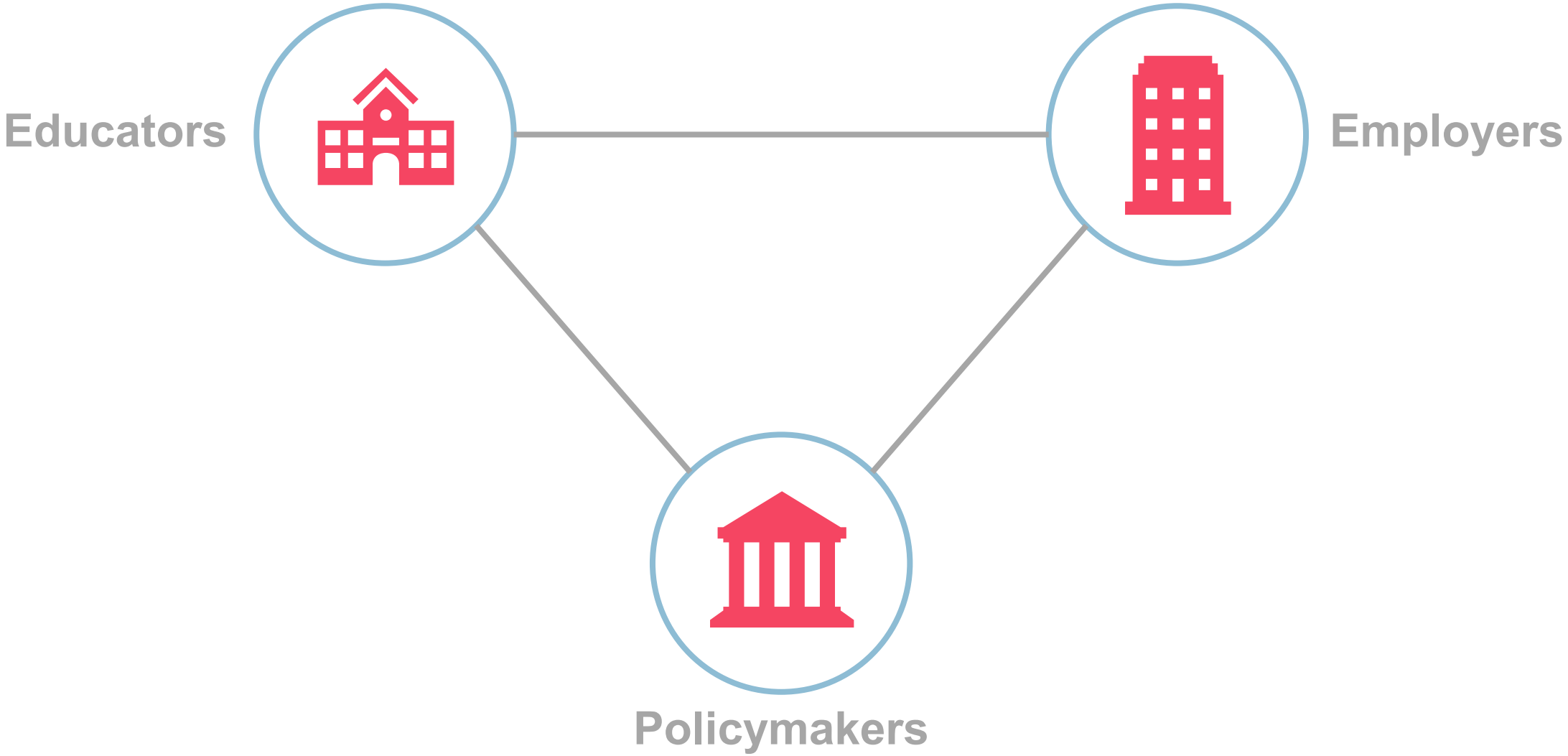
Building career pathways between skill-adjacent roles helps you:

- ✓ *Expand your talent pipeline*
- ✓ *Increase retention and employee engagement*
- ✓ *Reduce onboarding time*
- ✓ *Access more diverse pools of workers*



Find Others With Skin in the Game

Partner with Local Employers, Policymakers, and Training Providers to Build the Next Generation of Cybersecurity Workers



How Do We Make CyberSeek Even More Actionable for Federal Cybersecurity Employers?

Planned Enhancements to CyberSeek

1. Separate federal data from state and local governments in the tool
2. Include time series data to track historical cybersecurity demand, add breakouts by education and experience levels, and increase the number of certifications and training providers tracked in the tool
3. Provide sample job descriptions and other tools that help employers shift to skills-based hiring

Questions?

Contact Information:

Will Markow
Vice President of Applied Research - Talent
will.markow@lightcast.io

Learn More:

Lightcast.io

CyberSeek.org

FEDERAL CYBERSECURITY WORKFORCE WEBINAR

Q&A

Complete Evaluation Form

https://www.surveymonkey.com/r/Jan2023FedWebinar