HARNESSING THE POWER OF APPRENTICESHIP TO BRIDGE THE CYBERSECURITY WORKFORCE GAP

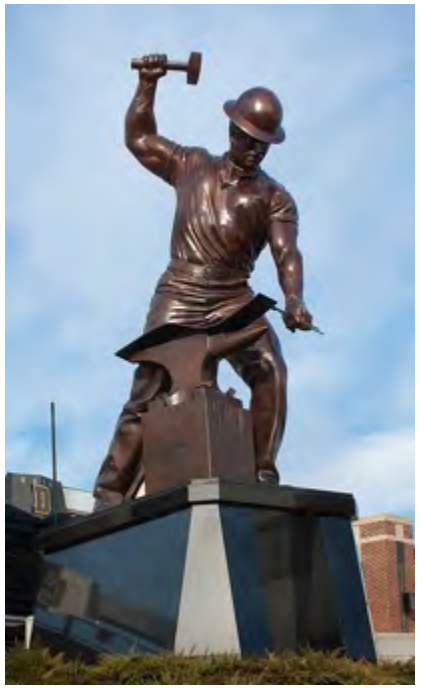
Strategies and Collaboration in Cyber Defense

PURDUE UNIVERSITY | cyberTAP

What is PCAP?

Purdue Cyber Apprenticeship Program

- Department of Labor funded program for scaling apprenticeships in key industry sectors, in this case cybersecurity
- “Earn and Learn”
- Connect public sector and industry partners with motivated individuals interested in cybersecurity
- Provide incumbent workers with a way to upskill and reskill their toolkits
- Address the cybersecurity workforce gap by offering quick-return hands-on training and education designed for working professionals

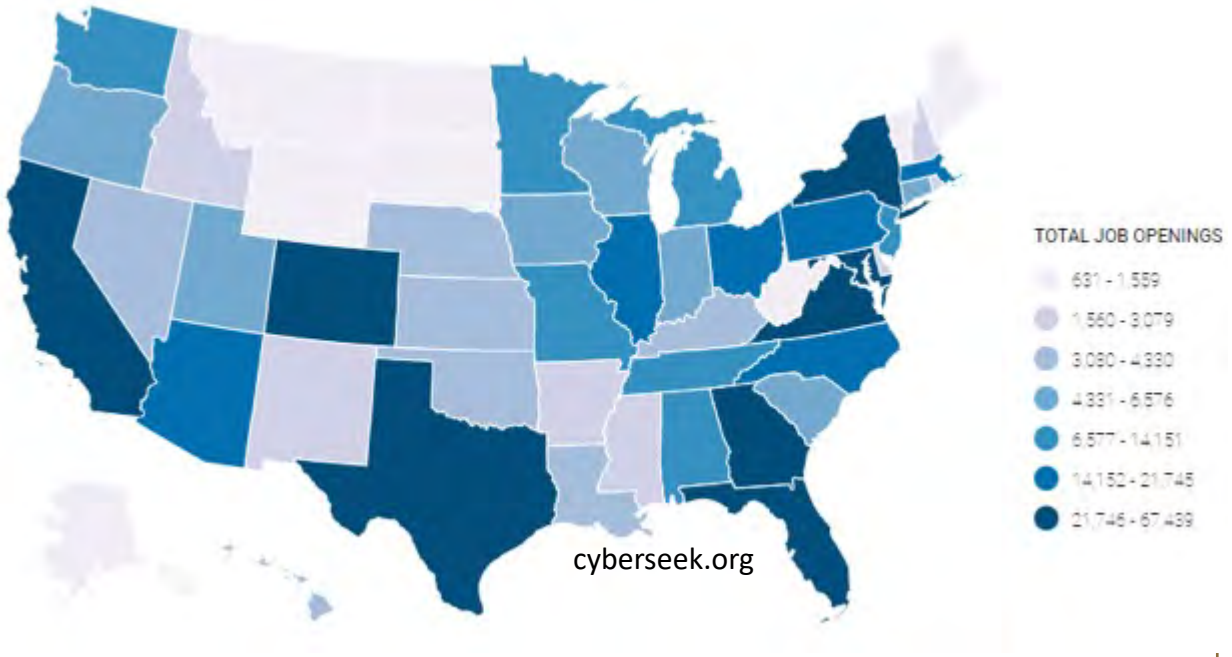


PURDUE UNIVERSITY | cyberTAP

Where is the workforce gap?

Yes, and a growing gap at that.

- Roughly 600,000 open cybersecurity jobs (up 20% from 2021)
- Nearly 40,000 open jobs in the public sector



PURDUE UNIVERSITY | cyberTAP

What does this mean for critical infrastructure?

Why am I here today…

- Colonial Pipeline
- Oldsmar, Florida Water Treatment Facility
- Ukraine/Russia conflict = increased threat activity
  - Power grid
  - Communications
  - Water/Wastewater
  - Transportation

What does this mean for critical infrastructure?

"A Rising Tide Lifts All Ships" – someone smarter than me

- Through this program we can reskill unemployed or underemployed individuals through direct training to spool-up the workforce
- Short-term, off-the-shelf curriculum allows for short lead-times and quick ROI
- Apprentices learn on the job so there is no gap in coverage
- We can start training at the speed of paperwork

5 Hallmarks of an Apprenticeship Program

What is required for each apprenticeship program?

- Paid/Work-Based Component
- OJT Training and Mentorship
- Educational and Instructional Component
- Industry-Recognized Credentials Earned
- Safety, Supervision, and Equal Employment Opportunity

Who can be an apprentice?

Apprentices…

- Must be a U.S. citizen, or be a green card holder
- Must be 18 years of age at the time of program enrollment
- Must be employed in an IT/cyber field, or have close proximity to an IT/cyber department within their organization
- Must NOT fund their own education (employer or PCAP funded)

What are the goals of PCAP?

Upskill and reskill the workforce

- We can upskill and reskill incumbent workers with minimal disruption to the workplace
- Cross-training employees can ensure vigilance across the organization, and provide cyber-awareness to parts of the organization that might otherwise be blind
- Provide an outlet for unemployed individuals who are interested in cybersecurity get a leg-up on other applicants through the PCAP Portal

Who is our Target Audience?

Purdue Cyber Apprenticeship Program - Services

Job-Seekers	Employed Individuals	Gov/Corp Partner
Registration into the PCAP Portal Complete assessments to quantify skill-level Front-row seat to prospective employers	Connect with employer to establish an apprenticeship program	Create program with existing employees --AND/OR-- Utilize the PCAP Portal to hand-select motivated prospects

Who is our Target Audience?

Private Sector Top Requested Job Titles (cyberseek.org)

- Cybersecurity Analyst
- Cybersecurity Manager
- Cybersecurity Consultant
- Software Developer
- Systems Engineer
- Network Engineer
- Penetration & Vulnerability Tester
- Systems Administrator
- Cybersecurity Specialist

Who is our Target Audience?

Public Sector

- cyberTAP is currently executing an NSA grant focused on adapting, creating, and assisting with the implementation of cybersecurity-related policy, procedures, tools, and training for local government and K-12 districts in Indiana

- Leverage local efforts as a test bed for scaling apprenticeship programs on a national level within the public sector, including critical infrastructure

- Apprenticeship programs can help local governments, municipalities, and public/private utilities tap into existing LOCAL talent pools that lack cybersecurity foundations

Off-the-Shelf Curriculum

A.C.E. Core Series

- Cohort or Individual
- Asynchronous remote delivery
- Geared towards beginner and intermediate learners
- 40 content hours for each course

Cybersecurity Foundations

Learn the basic principles of cyber and information security. Topics covered include general cyber domain knowledge, key security concepts, risk & vulnerability management, cryptography basics, and identity access management.

Duration:	Virtual Labs:
4 weeks	7 labs

Enterprise Security

Learn what it takes to create, implement, and manage enterprise-level security efforts. Topics include security frameworks, network architecture, protocols, wireless security, monitoring, virtualization and cloud, basics of malware, data protection, and more.

Duration:	Virtual Labs:
4 weeks	7 labs

Vulnerability Management

Learn about the basics of vulnerability concepts and analysis. Topics covered include threat hunting, vulnerability scanning & reporting, incident response, disaster recovery, application security, and more.

Duration:	Virtual Labs:
4 weeks	7 labs

Ethical Hacking

Learn the foundations for ethical hacking through videos, readings, and labs. Topics covered include the basics of ethical hacking, network and systems enumeration, vulnerability scanning, system attacks, sniffing, and social engineering.

Duration:	Virtual Labs:
4 Weeks	7 labs

PURDUE UNIVERSITY | cyberTAP

Off-the-Shelf Curriculum

A.C.E. Defender

- Cohort or Individual
- Focuses on blue-team, defensive security operation skills
- Remote delivery
- Geared towards experienced cyber professionals
- 16 content hours for each course

Security Operations 1

Learn security operations and defensive security, including the basics of Windows, Linux, and network forensics. Key concepts and tools include commercial SIEM, firewalls, and systems monitoring.

Duration:	Range Hours:	
2 days	6 hours	3 scenarios

Security Operations 2

Continue learning key defensive security concepts, including Linux and Windows log management, scripting, packet sniffing, and more. Key concepts and tools include commercials SIEMs and firewalls, and other investigation tools.

Duration:	Range Hours:	
2 days	9 hours	3 scenarios

Security Operations 3

Continue learning key defensive security concepts, including Linux log management, Windows and Linux forensics, and MS SQL technologies. Key concepts and tools include commercials SIEMs and firewalls, common mail server applications, packet capture tools.

Duration:	Range Hours:	
2 Days	10 hours	3 scenarios

Security Operations 4

Finish key learning objectives of defensive security concepts including advanced Linux and Windows forensics and logging, reverse engineering techniques. Key concepts and tools include commercials SIEMs and firewalls, and other investigation tools.

Duration:	Range Hours:	
2 Days	12 hours	3 scenarios

PURDUE UNIVERSITY | cyberTAP

Off-the-Shelf Curriculum

A.C.E. Raider

- Cohort or Individual
- Focuses on red-team, offensive security operation skills
- Remote delivery
- Geared towards experienced cyber professionals
- 16 content hours for each course

PURDUE UNIVERSITY | cyberTAP

How to Engage…

Two Primary Paths: Individual or Corporation

- Corporate and Government Partners:
  - Contact me: stratton@purdue.edu
    - MOA to establish partnership, and acknowledgement of “5 hallmarks”
    - SOW to define educational and OJT component
    - Individual intake of apprentices
- Employed Individuals
  - Visit our website: purdue.edu/pcap
- Job-Seeking Individuals
  - Visit the PCAP Portal: purdue.edu/pcap/portal

THANK YOU

stratton@purdue.edu

cyber.tap.purdue.edu

purdue.edu/pcap

PURDUE UNIVERSITY | cyberTAP