



CYBERPATRIOT

THE AIR FORCE ASSOCIATION'S
NATIONAL YOUTH CYBER EDUCATION PROGRAM

EXTRA TRAINING – DAY 1

Cybersecurity Career Path



Learning Objectives

- Career Path
 - Cybersecurity Color Wheel and Industry Segments
 - Career Sites to Get Started With
 - Using LinkedIn and Related Tools
 - Beyond AFA CyberPatriot
- Five Recommendations for Advancing Careers
 - Learning AI Skills
 - Develop Programming Skills
 - Understand Virtualization Techniques
 - Learn Cloud Skills
 - Understand the Business Intersection



CYBERPATRIOT

THE AIR FORCE ASSOCIATION'S
NATIONAL YOUTH CYBER EDUCATION PROGRAM

DAY 1 - SECTION 1

Developing Your Career Path



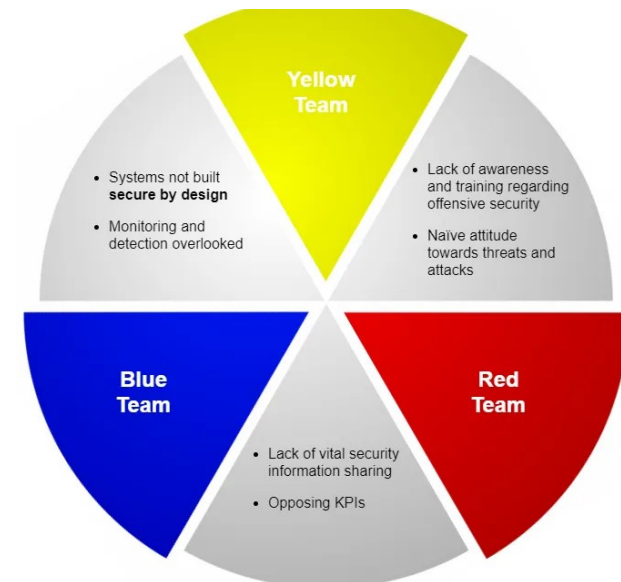
Cyber Color Wheel

- Representative of Cybersecurity Focus Areas
 - Method of identifying the purpose of a team/individual based on an association with a particular colors
 - Identified gaps in mindsets among different silos of operation
 - Developed a common terminology setting
- Newer Concept – 2017
 - Presented at BlackHat as a method of classifying jobs
 - First presented by April Wright
 - Expanded by Louis Cremen in 2020
- Color Definitions
 - Primary Colors: base functions separate from other jobs
 - Secondary Colors: cooperative overlaps
 - Center (White): overview and management practices



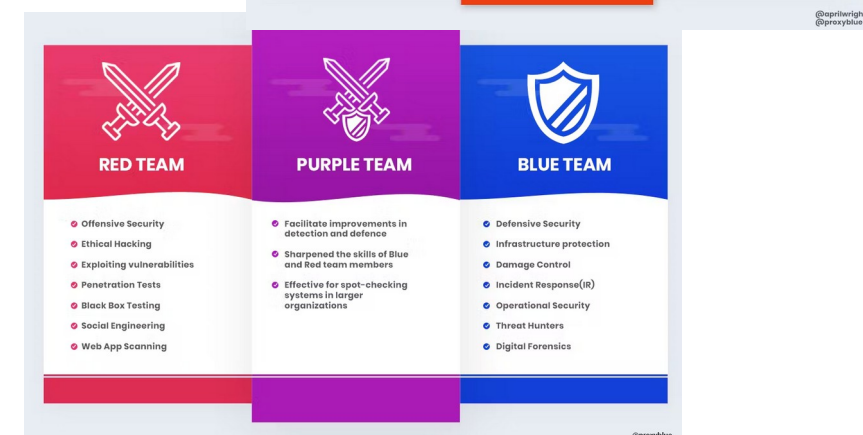
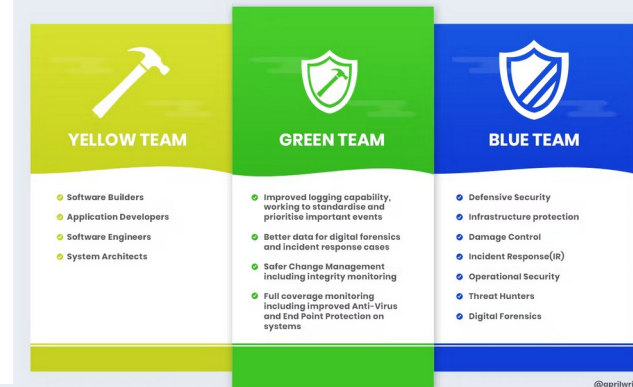
Cyber Color Wheel – Primary

- **Blue Team: (Defenders)** responsible for the defense of the enterprise systems and environments
- **Red Team: (Attackers)** responsible for identifying and finding risks, issues and vulnerabilities with the enterprise systems and applications
- **Yellow Team: (Builders)** development and coders responsible for designing and building software
- **White Team: (GRC)** responsible for the oversight and policy management of the cybersecurity program



Cyber Color Wheel – Secondary

- **Green Team:** responsible for code development focused on closing the gaps in defensive security operations. Look at aspects like logging and monitoring, encryption, identity interfaces and securing APIs.
- **Orange Team:** responsible for working with code development teams to close gaps related to attacking software operations, validating test scenarios and making code more secure.
- **Purple Team:** cooperative teams responsible for working with defenders and attackers to identify practices and methods of working together.



Cybersecurity and Infrastructure Security Agency (CISA)



America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

How can we help?



[Find Help Locally](#)

[Contact your Region](#)

[Assist Visits](#)

[Protected Critical Infrastructure Information](#)



[Industry](#)

[Secure by Design](#)

[Information Sharing: A Vital Resource](#)

[PCI Program modernized](#)

[Joint Cyber Defense Collaborative expands](#)



[Small and Medium Businesses](#)

[Cyber guidance for small businesses](#)

[Supplementing passwords](#)

[Doing business with CISA](#)



[Educational Institutions](#)

[School Safety](#)

[Cybersecurity for K-12](#)

[K-12 School Security Product Suite](#)

[Protecting Our Future: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats](#)

Additional CISA Resources



[CISA's Federal Cyber Defense Skilling Academy](#)

CISA's Federal Cyber Defense Skilling Academy provides full-time federal employees an opportunity to focus on professional growth through an intense, full-time, three-month accelerated training program.



[CISA Events](#)

CISA hosts and participates in events throughout the year to engage stakeholders, seek research partners, and communicate with the public to help protect the homeland.



[CISA Services Catalog](#)

A single resource that provides you with access to information on services across CISA's mission areas.



[CISA Training](#)

As part of our continuing mission to reduce cybersecurity and physical security risk, CISA provides a robust offering of cybersecurity and critical infrastructure training opportunities.

- Agency managed under Department of Homeland Security (DHS)
- **America's CISO**
- Services are available to public and private sector organizations
- Cybersecurity Training available
 - Free training
 - OT/IT Systems
 - Agency paid training academy
- Cybersecurity assessment
- NIST Frameworks use and promotion
- Known Exploit Vulnerability Catalog

Cybersecurity and Infrastructure Security Agency (CISA)



America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

- 41 Defined Job Roles
- Some have sub-specialties
- Categorized into five different focus areas
- Data available at CISA > Career Pathways
 - <https://niccs.cisa.gov/tools/cyber-career-pathways-tool>
 - <https://niccs.cisa.gov/tools/nice-framework>



Try Cyber

SELECT CHALLENGE

Network Operations

Technical Challenge | Difficulty: ☆

Assist with adding additional IP addresses to a server's network interface. [NICE Framework T1314]



Technical Support

Technical Challenge | Difficulty: ☆

Assist with provisioning new user accounts on a system for new employees. [NICE Framework T1569]



Database Administration

Technical Challenge | Difficulty: ☆ ☆

Assist with setting up a new database by importing backups from another database. [NICE Framework T1240]



Incident Response

Technical Challenge | Difficulty: ☆ ☆

Help collect intrusion artifacts from packet captures containing evidence of a cyber-attack. [NICE Framework T1370]



Systems Security Analysis

Technical Challenge | Difficulty: ☆ ☆

Assist with applying a security policy to a client's workstation. [NICE Framework T1076]



Vulnerability Analysis

Technical Challenge | Difficulty: ☆ ☆

Help perform a security audit on an organization's workstations. [NICE Framework T1619]



Defensive Cybersecurity

Technical Challenge | Difficulty: ☆ ☆ ☆

Assist with analyzing suspicious network traffic and identifying threats. [NICE Framework T1084, T0185]



Systems Administration

Technical Challenge | Difficulty: ☆

Assist with managing system privileges by adding users to privileged groups. [NICE Framework T1569]



Data Analysis

Technical Challenge | Difficulty: ☆ ☆

Help identify troubling trends in the intrusion prevention software's logs. [NICE Framework T0349]



Digital Evidence Analysis

Technical Challenge | Difficulty: ☆ ☆

Help scan digital evidence for malicious software. [NICE Framework T1381]



Systems Administration Adv.

Technical Challenge | Difficulty: ☆ ☆

Help install software on a new web server for a company's web developers. [NICE Framework T1500]



Technical Support Adv.

Technical Challenge | Difficulty: ☆ ☆

Help resolve support tickets related to locked user accounts. [NICE Framework T1538]



Database Administration Adv.

Technical Challenge | Difficulty: ☆ ☆ ☆

Assist with configuring a new database management system for a company's application developers. [NICE Framework T1565]



Network Operations Adv.

Technical Challenge | Difficulty: ☆ ☆ ☆

Help diagnose and resolve a server's networking configuration issues. [NICE Framework T0081]

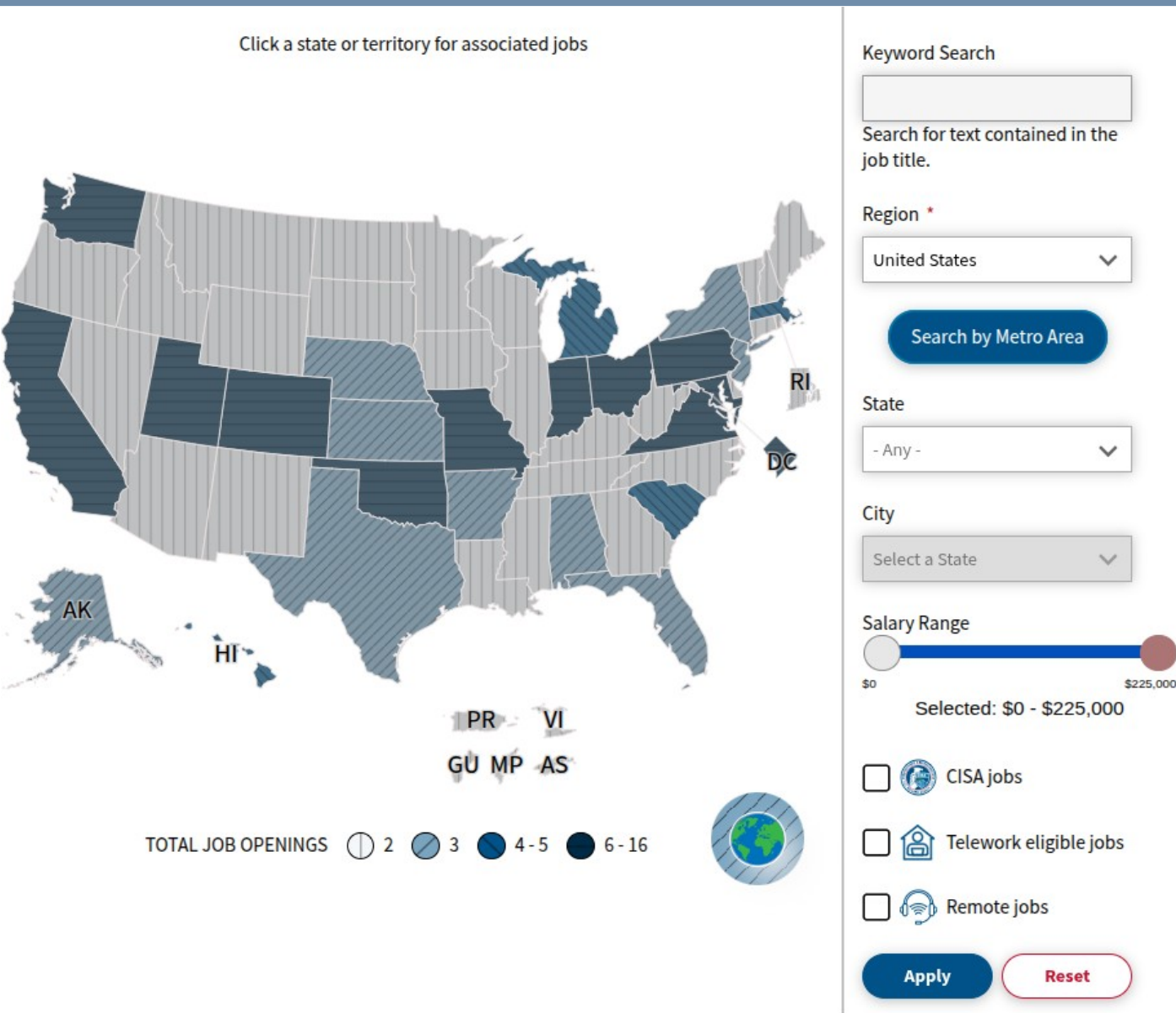


- Interactive site focused on performing micro-challenges to help users identify passions and abilities
- 14 areas of exploration
- Allows for individuals to try different scenario based activities to determine if the role is worth pursuing
- Selectable levels of interaction based on previous experience – varying levels of difficulty involved





<https://trycyber.us/challenges/>

Cybersecurity and Infrastructure Security Agency (CISA)

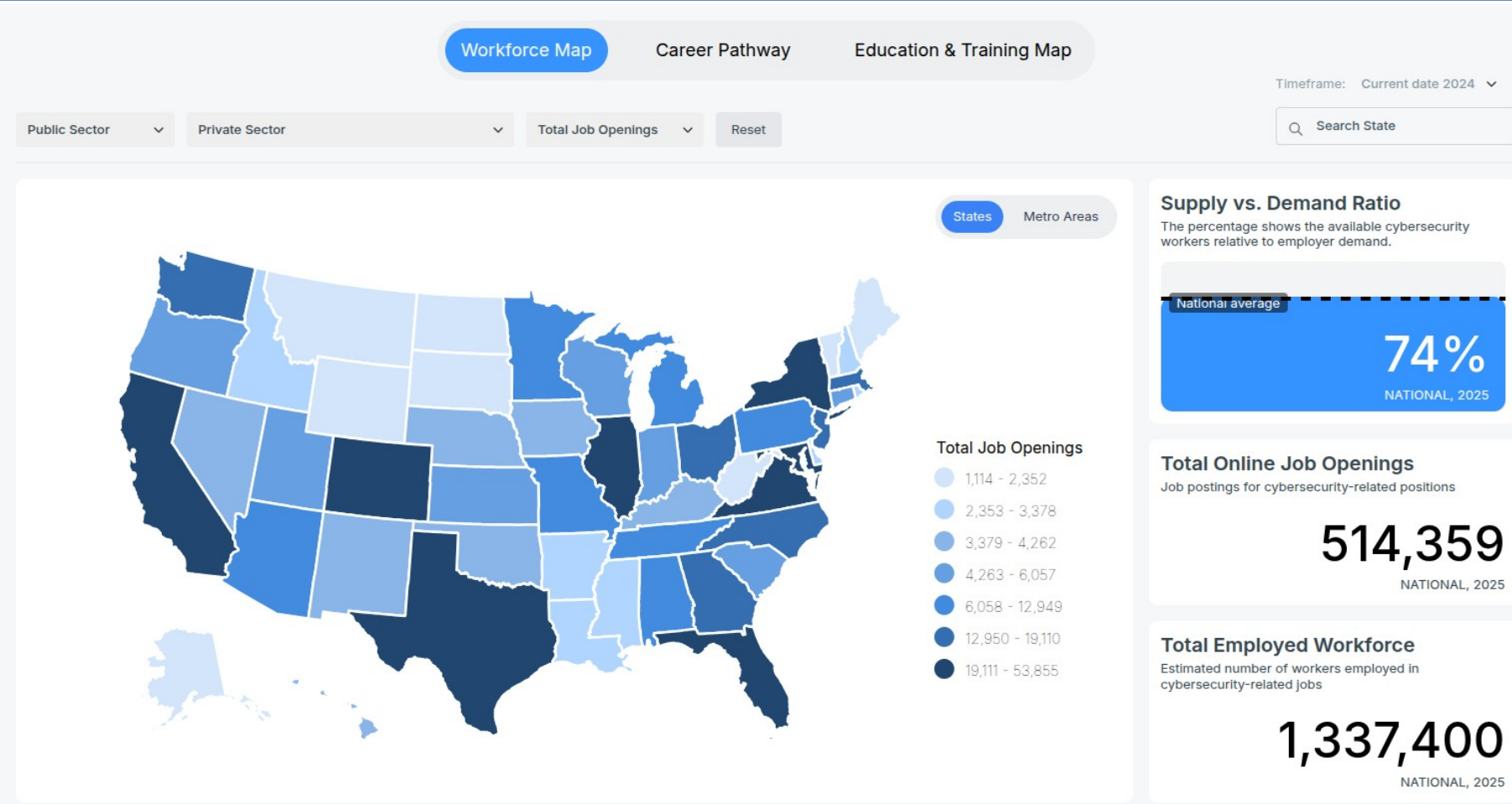


- Interactive site focused identifying possible federal jobs and associated salary ranges
- Selectable by state, agency, type ...
- Allows for selectability to position types, metro locations, keyword search by title

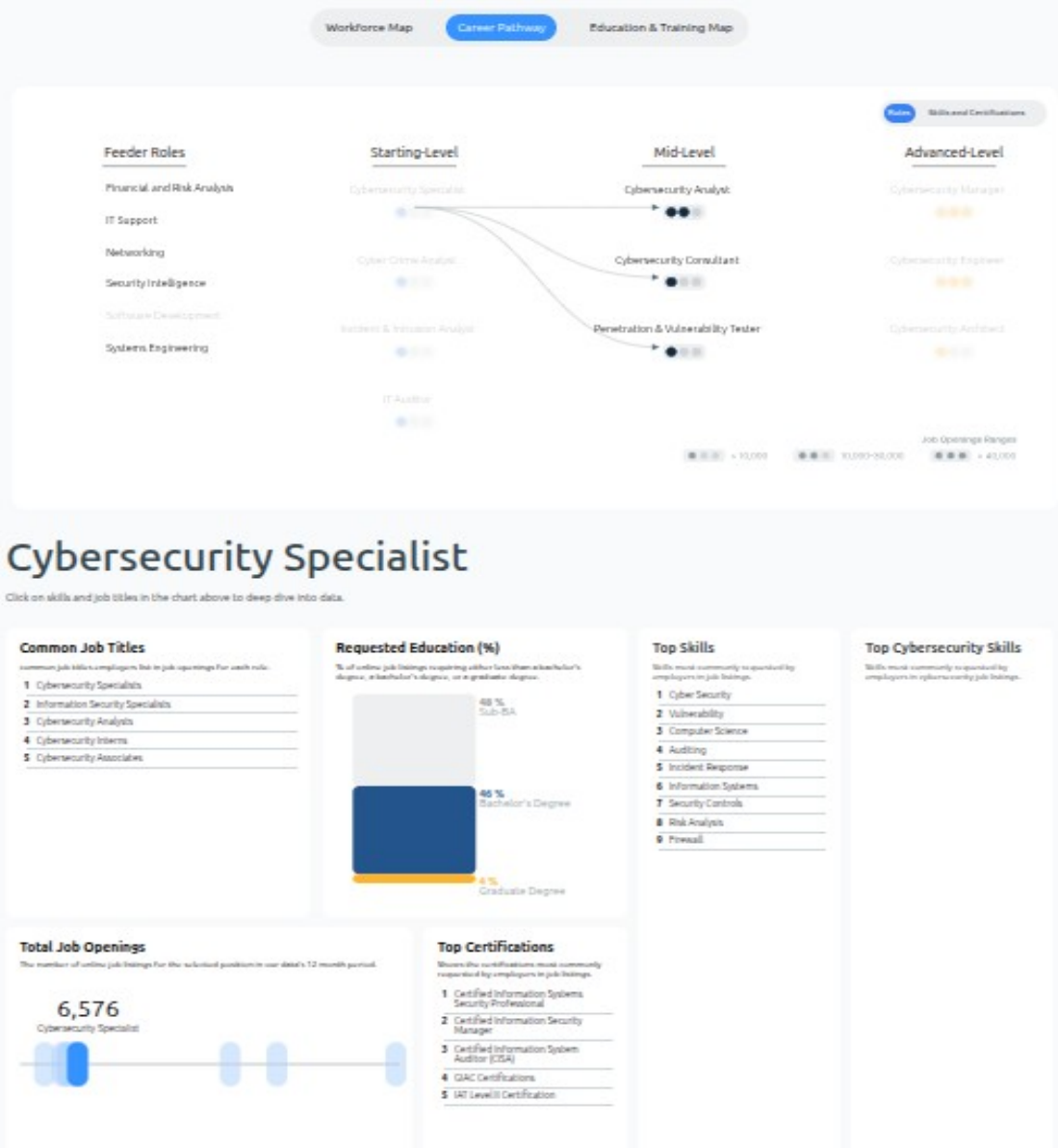
Cybersecurity and Infrastructure Security Agency (CISA)

Title	City	State	Minimum	Maximum	Apply By
Information Technology Specialist (CUSTSPT) - 840601300	Elmendorf AFB	Alaska	\$27 Per Hour	\$33 Per Hour	07/28/2025
Biomedical Equipment Support Specialist - 840318900	Tulsa	Oklahoma	\$40,332	\$127,267	07/30/2025
Biomedical Equipment Support Specialist - 840318500	Tulsa	Oklahoma	\$40,332	\$127,267	07/30/2025
 Interdisciplinary Engineer - 838036600	McClellan	California	\$44,708	\$106,543	07/15/2025
 Public Notice for Information Technology Cybersecurity Specialist (Direct Hire) - 689241200	1143 Cities	56 States and/or Territories	\$47,813	\$155,403	09/22/2025
Bio Equip Support Spec - 839713400	2 Cities	Massachusetts	\$48,236	\$114,951	09/01/2025
Bio Equip Support Spec - 839713300	2 Cities	Massachusetts	\$48,236	\$114,951	09/01/2025
Biomedical Equipment Support Specialist - 839890300	Aurora	Colorado	\$55,471	\$128,088	03/11/2026
Biomedical Equipment Support Specialist - 839890400	Aurora	Colorado	\$55,471	\$128,088	03/11/2026
Biomedical Equipment Support Specialist - 839891300	Aurora	Colorado	\$55,471	\$128,088	03/11/2026
 Public Notice for Computer Scientist - Cybersecurity (Direct Hire) - 689240500	1143 Cities	56 States and/or Territories	\$57,442	\$155,403	09/22/2025
HR SPEC (MILITARY) (Title 32) - 839622100	Fort Smith	Arkansas	\$61,111	\$79,443	07/14/2025
 IT Cybersecurity Specialist (CUSTSPT) - 840597100	Norfolk	Virginia	\$62,020	\$80,624	07/15/2025

- Interactive site focused identifying possible jobs and salary ranges
- 14 areas of exploration
- Allows for individuals to try different scenario based activities to determine if the role is worth pursuing
- Selectable levels of interaction based on previous experience – varying levels of difficulty involved



- Interactive dashboard map showing potential job opening and salary ranges for private and non-profit sector
- Three areas of display opportunity – Workforce / Career Pathway/ Education Opportunities
- Selectable levels of interaction based on location



- Selectable pathways to various roles, including:
 - Entry pathways to the role
 - Beginning / Mid-career / Advanced Career
 - Various upward mobility paths
- Expected salary ranges – National and local level
- Expected job openings for the given specialty
- Required skills to work on
- Associated certifications related to this role

Bureau of Labor and Statistics

- Occupational Outlook Handbook is a wealth of knowledge related to career pathing
- Standardized categorization of job codes
- Multiple tab selection to narrow in, including:
 - Pay Scales – National and local
 - Education and training requirements
 - Job descriptions
 - Job outlook for selected role – national and local
- Comparative roles

<https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-1>

U.S. BUREAU OF LABOR STATISTICS

Search BLS.gov

HOME SUBJECTS DATA TOOLS PUBLICATIONS ECONOMIC RELEASES CLASSROOM BETA

Bureau of Labor Statistics > Publications > Occupational Outlook Handbook > Computer and Information Technology

OOH HOME OCCUPATION FINDER OOH FAQ HOW TO FIND A JOB A-Z INDEX OOH SITE MAP

OCCUPATIONAL OUTLOOK HANDBOOK

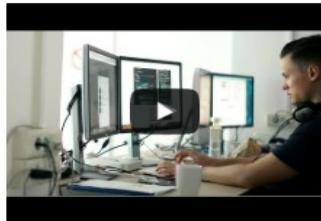
Search Handbook Go

Information Security Analysts

Summary What They Do Work Environment How to Become One Pay Job Outlook State & Area Data Similar Occupations More Info

Summary

Quick Facts: Information Security Analysts	
2024 Median Pay	\$124,910 per year \$60.05 per hour
Typical Entry-Level Education	Bachelor's degree
Work Experience in a Related Occupation	Less than 5 years
On-the-job Training	None
Number of Jobs, 2023	180,700
Job Outlook, 2023-33	33% (Much faster than average)
Employment Change, 2023-33	59,100



What Information Security Analysts Do
Information security analysts plan and carry out security measures to protect an organization's computer networks and systems.

Work Environment
Most information security analysts work for computer companies, consulting firms, or business and financial companies.

How to Become an Information Security Analyst
Information security analysts typically need a bachelor's degree in a computer science field, along with related work experience. Employers may prefer to hire analysts who have professional certification.

Pay
The median annual wage for information security analysts was \$124,910 in May 2024.

Job Outlook
Employment of information security analysts is projected to grow 33 percent from 2023 to 2033, much faster than the average for all occupations.
About 17,300 openings for information security analysts are projected each year, on average, over the decade. Many of those openings are expected to result from the need to replace workers who transfer to different occupations or exit the labor force, such as to retire.

State & Area Data
Explore resources for employment and wages by state and area for information security analysts.

Similar Occupations
Compare the job duties, education, job growth, and pay of information security analysts with similar occupations.

More Information, Including Links to O*NET
Learn more about information security analysts by visiting additional resources, including O*NET, a source on key characteristics of workers and occupations.

Bureau of Labor and Statistics – O*NET Online

- Selectable to localization, including:
 - Compares national to state/local differences
 - Salary range per Metro
 - All links are clickable
- Approximate number of job opportunities available per metro location



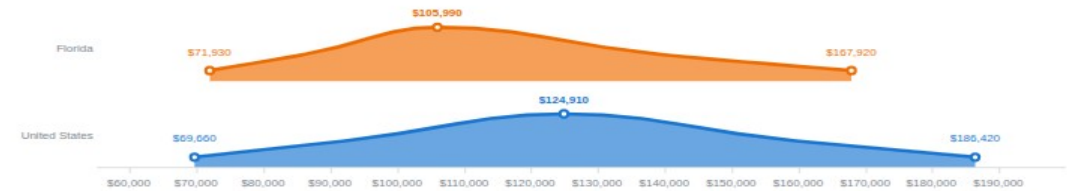
Florida Wages

15-1212.00 - [Information Security Analysts](#) Bright Outlook

Wages for state: Florida Go

Wages near ZIP Code: Go

Annual Wages Hourly Wages



In Florida:

- Workers on average earn **\$105,990**.
- 10% of workers earn **\$71,930 or less**.
- 10% of workers earn **\$167,920 or more**.

In the United States:

- Workers on average earn **\$124,910**.
- 10% of workers earn **\$69,660 or less**.
- 10% of workers earn **\$186,420 or more**.

Source: Bureau of Labor Statistics [2024 wage data](#) [us](#)

Full Details

Save Table: [XLSX](#) [CSV](#)

Location	Annual Low (10%)	Annual Q _L (25%)	Annual Median (50%)	Annual Q _U (75%)	Annual High (90%)
United States	\$69,660	\$92,160	\$124,910	\$159,600	\$186,420
Florida	\$71,930	\$86,250	\$105,990	\$139,150	\$167,920
Cape Coral-Fort Myers, FL	\$67,530	\$85,290	\$103,680	\$134,690	\$163,530
Crestview-Fort Walton Beach-Destin, FL	\$80,310	\$99,270	\$107,670	\$131,360	\$164,580
Deltona-Daytona Beach-Ormond Beach, FL	\$55,580	\$70,110	\$94,030	\$126,660	\$151,450
Gainesville, FL	\$71,420	\$93,310	\$102,330	\$117,020	\$129,540
Jacksonville, FL	\$70,710	\$82,340	\$103,620	\$136,260	\$162,700
Lakeland-Winter Haven, FL	\$60,550	\$77,780	\$97,190	\$128,260	\$157,890
Miami-Fort Lauderdale-West Palm	\$70,800	\$91,450	\$107,260	\$137,250	\$170,770

<https://www.onetonline.org/link/localwages/15-1212.00?st=FL>

Cyber Career Opportunities

- 1. Security Software Developer:** software is often not built with security in mind. The Security Software Developer designs and integrates security into every aspect of the software development lifecycle.
- 2. Security Architect Career Path:** Create and build secure networks and computers for complex security frameworks. This is an ideal career path for the problem solver who enjoys solving puzzles.
- 3. Security Consultant:** Experts that evaluate cybersecurity threats, risks and problems to guide organizations in providing protection solutions. This is a very tech-savvy position.
- 4. Information Security Analyst:** Professionals that stand at the front line of defense for networks. They create and maintain firewalls and monitor network activities.
- 5. Ethical Hacker:** Are licensed professionals that try to hack a network with permission to find vulnerabilities. They try to find what is vulnerable and could be exploited by a malicious hacker.
- 6. Computer Forensics Analyst:** Professionals that focus on cyber crimes and partake in data recovery, intercepting data linked to crimes, and a detailed look into data trails.
- 7. Chief Information Security Officer:** Mid Executive position that oversees an organization's IT department. They are responsible for planning, managing, and directing all computer, network and data security needs.
- 8. Penetration Tester:** Highly skilled professionals that are typically ethical hackers and try to infiltrate a corporation's security measures (physical and electronic) with permission from the corporation. A penetration tester will use social engineering tactics to test the security of a company's employee practices.
- 9. IT Security Consultant:** Are typically outsourced contractors that advise organizations on cybersecurity objectives. They typically service smaller businesses on tighter budgets.
- 10. Security Systems Administrator:** The person in charge of daily operations for security controls (installing, administering, maintaining, and troubleshooting) to include backing up data, network monitoring, user account management, and general security needs.

Source: <https://medium.com/@coderacademy/10-careers-in-cyber-security-you-should-consider-2613061a8cb2>

Using LinkedIn

Social Media Landscape 2023



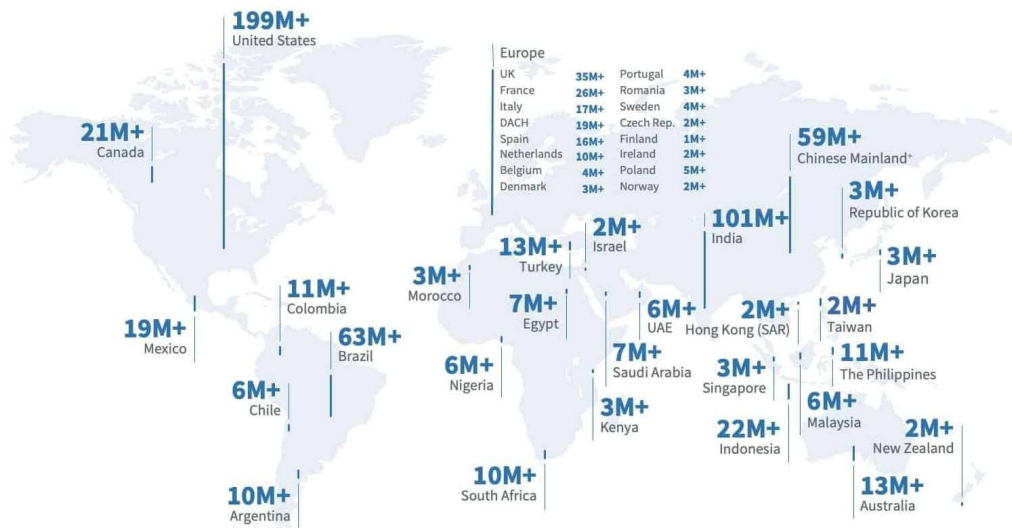
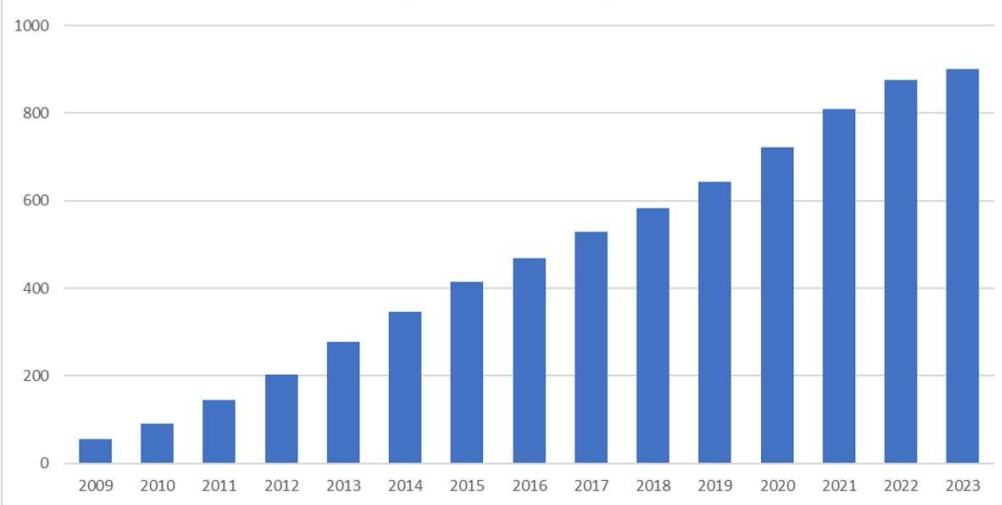
Social Media is very prevalent in today's society and is accepted both in and out of the workplace

Social Media is a continuum. Several “services” may cross the lines between areas of focus

- [Focused on Establishing Conversations:](#)
- posting information and articles; microblogs and tweets
- [Focused on Sharing:](#) video sharing and
- streaming sites, photo sharing, video snippets
- [Focus on Publishing:](#) blogging sites;
- collaboration; ratings and reviews
- [Focused on Participation:](#) gaming sites;
- virtual worlds

Using LinkedIn

LinkedIn Members Worldwide - 2009 - 2023
(Shown in Millions)



Platform information: (12/2023)

- Total Number of LinkedIn Users: 900+ million
- Total Number of LinkedIn Users from the US: 199+ million
- Percentage of LinkedIn Monthly Active Users: 46.97%

Demographics:

- More than 75% of LinkedIn users are from outside the US
- 59% of LinkedIn Users are 25-34 years old & 20% of 18-24 years old
- 50% of internet users with a college degree or higher use LinkedIn
- 29% of US adults are signed up to use LinkedIn

Interesting Facts:

- More than 95% of US recruiters use LinkedIn regularly
- 59% of LinkedIn members have never worked at a company with more than 200 employees
- 2 million posts, articles, and videos are published on LinkedIn every day
- There are 100 million job applications on LinkedIn every month
- Only ~3 million LinkedIn users share content on a weekly basis

Using LinkedIn

Building a Professional Network:

- Making connections
- Finding people you know, and who they know ...
- Not just about quantity - quality connections

Industry/ Professional Updates:

- What's new & exciting in [your] industry or specialty
- What are the hot topics that professionals are discussing
- Who should I be following?

Finding a Job/ Getting Promoted

- Searching for Job Postings for advancement
- Researching Companies and Industries
- Researching salary information and like positions
- Researching people to talk to - find mentors

All About Branding !

Your profile and how you use it speaks to the marketing brand that you want to promote for yourself in the professional setting.

You are your own best marketing agency.:

- ***What story do you want to tell?***
- What image of you are you selling?
- What's important to you?
- What you like and share has meaning
- How do you want current and potential employers to feel about you?

How you show up in searches and in activity depends on how you set it up and use it.



CYBERPATRIOT

THE AIR FORCE ASSOCIATION'S
NATIONAL YOUTH CYBER EDUCATION PROGRAM

DAY 1 - SECTION 2

Top Recommendations to Advance in Cyber



Top Five Skills Recommendations

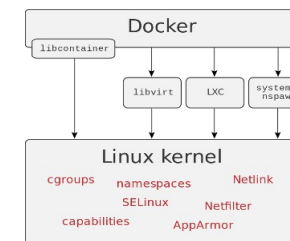
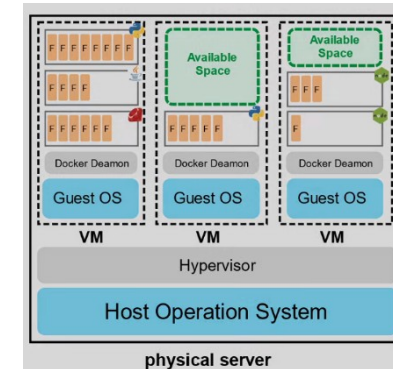
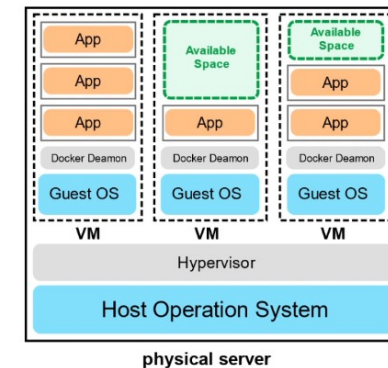
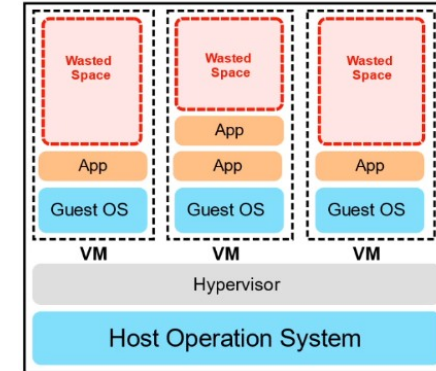
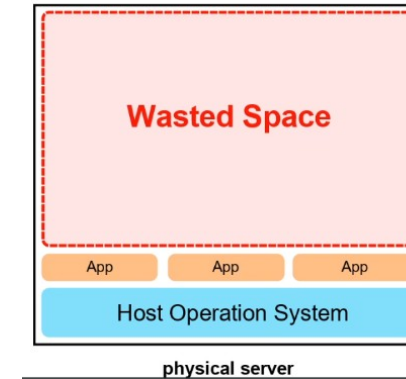
- IT and Cybersecurity are rapidly advancing careers in technology. The pace of change in technology is staggering in today's world.
- Some recommendations to consider:
 1. Understand **virtualization** of technology
 2. Learn some **programming**
 3. Develop **skills with AI** Technology
 4. Understand **cloud** technologies
 5. Develop **business skills** | Understand business intersection

Understanding Technology Virtualization

- The change from physical to virtual technology have advanced significantly for the last 10+ years.
- Some concepts to consider:
 - Use of [VMWare WorkStation](#) | [VirtualBox](#)
 - Multiple hypervisors available – [Microsoft](#) (WSL, Hyper-V) and [Linux](#) variants
 - [Docker containerization](#) is a different method of virtualizing software – whole or parts

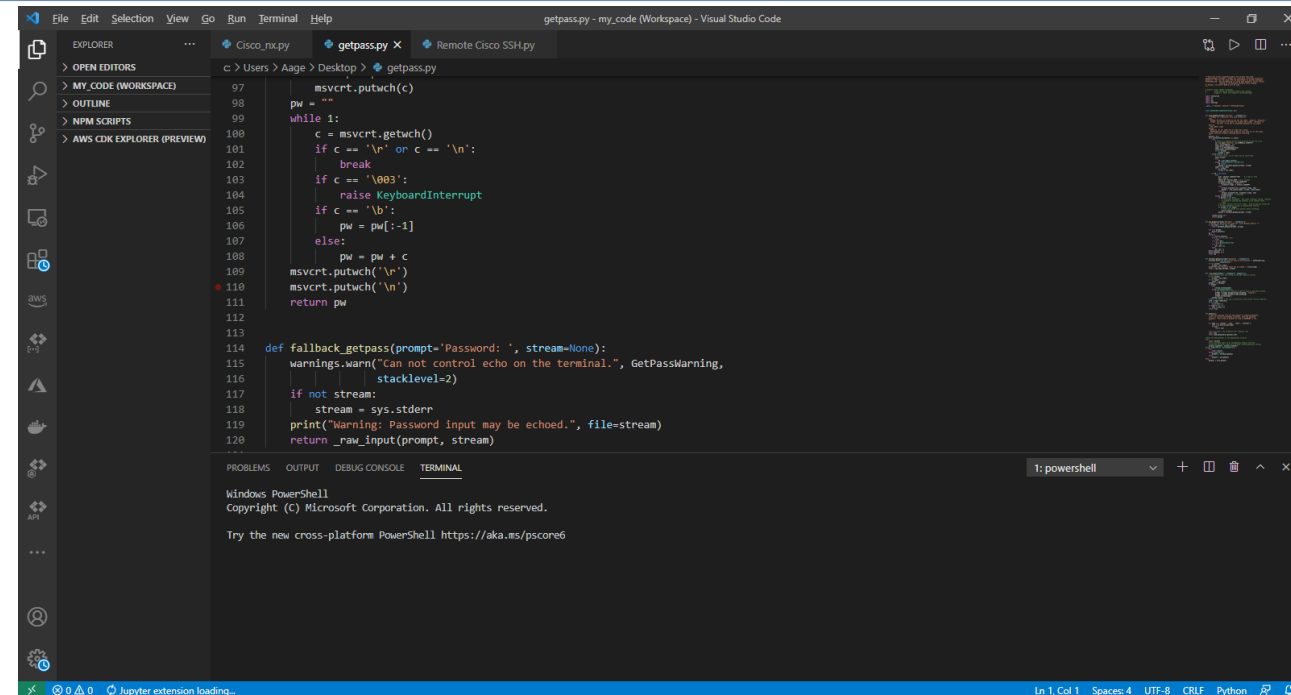
Manages memory and available resources among the varied GUEST VMs

Blade servers and independent systems – headless and autonomous



Develop Programming Skills

- You do not need to code to have or use programming skills to be able to understand how code works or what it does
- Some concepts to consider:
 - 1 Learn to use **Python** programming – a scripting language
 - 2 Regardless of what IT/Cyber area, scripting languages are used for building automation processes
 - 3 Understanding Waterfall and Agile programming techniques
 - 4 DEVOPS & DEVSECOPS are current programs focused around continuous code development and deployment (CI/CD)



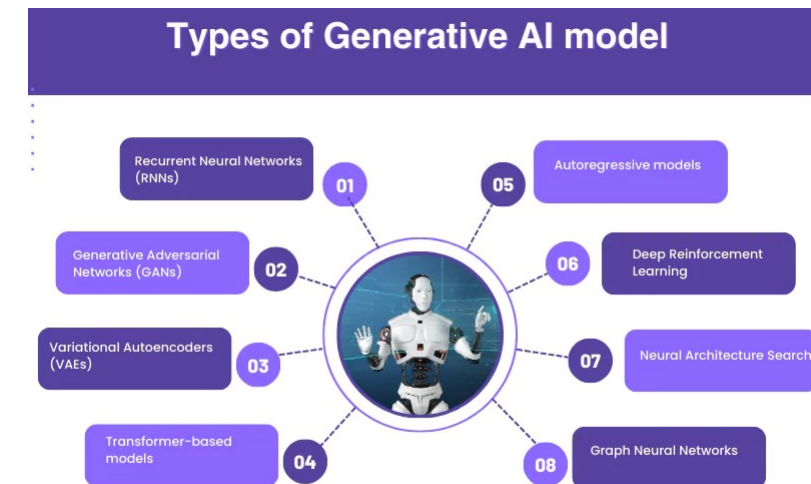
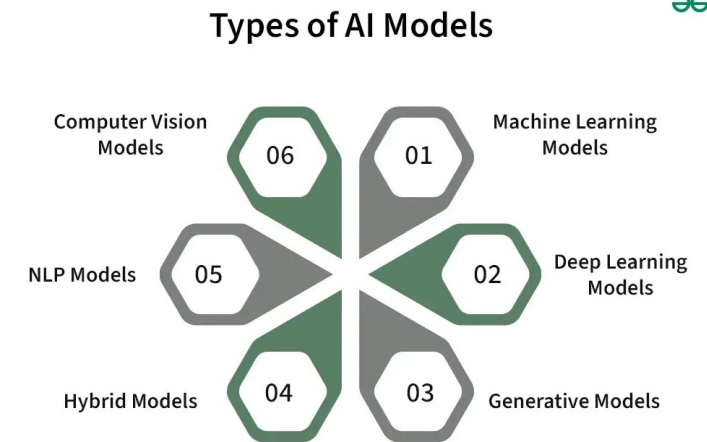
The screenshot shows the Visual Studio Code interface. The Explorer pane on the left shows the file structure with 'getpass.py' selected. The main editor area displays the code for 'getpass.py', which includes a password prompt function and a fallback function. The terminal at the bottom shows the Windows PowerShell prompt.

```
97 msvcrt.putwch(c)
98 pw = ""
99 while 1:
100     c = msvcrt.getwch()
101     if c == '\n' or c == '\n':
102         break
103     if c == '\003':
104         raise KeyboardInterrupt
105     if c == '\b':
106         pw = pw[:-1]
107     else:
108         pw = pw + c
109     msvcrt.putwch('\n')
110     msvcrt.putwch('\n')
111     return pw
112
113
114 def fallback_getpass(prompt='Password: ', stream=None):
115     warnings.warn("Can not control echo on the terminal.", GetPassWarning,
116                 stacklevel=2)
117     if not stream:
118         stream = sys.stderr
119     print("Warning: Password input may be echoed.", file=stream)
120     return _raw_input(prompt, stream)
```



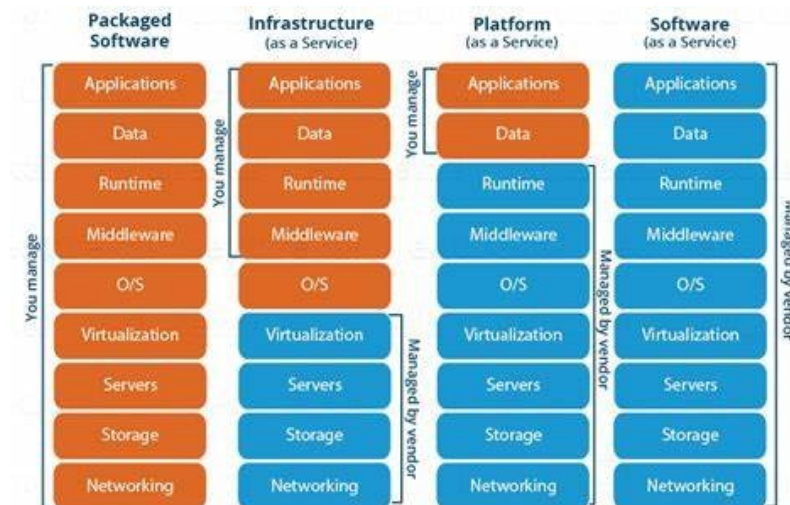
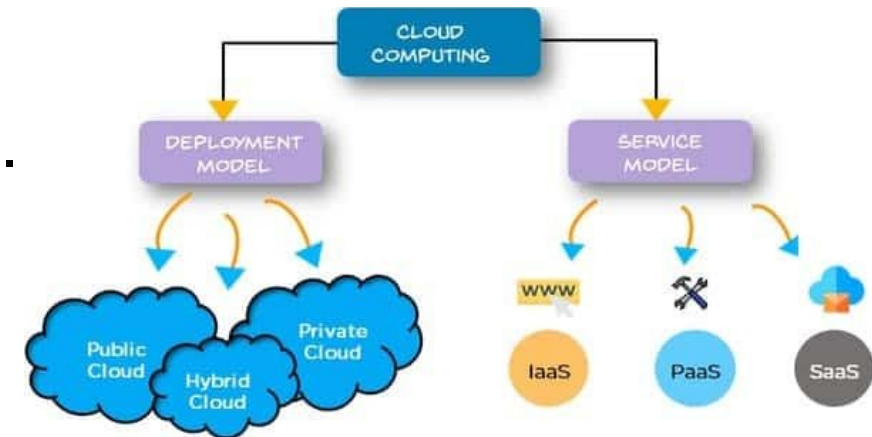
Learn about Artificial Intelligence (AI)

- IT and Cybersecurity are rapidly advancing careers in technology. The pace of change in technology is staggering in today's world.
- **AI** is a leading driver of change
- Some recommendations to consider:
 - 1 Understand what **LLMs** are
 - 2 Gain some **prompting** experience
 - 3 Develop **AI security skills**
 - 4 Understand **predictive** and **generative** technologies



Understand Cloud Technologies

- Cloud technology and its use continues to grow, and grow more important within the scope of technologists. Start-ups/newer orgs rely on it more heavily than traditional companies.
- Some concepts to consider:
 - 1 Cloud is more than “just someone else’s computer ...”
 - 2 Cloud operations come in three modes: IaaS / PaaS / SaaS
 - 3 Major cloud companies are Microsoft, Amazon and Google
 - 4 Not everything running in the cloud relies on a server
 - 5 Maintaining Cybersecurity in the cloud can be much different
 - 6 [Free training](#) is available for each platform



Get Business Skills

- IT and Cybersecurity do not exist for the sake of just using technology. There is almost always a business need behind it.
- Some business skill recommendations to consider:
 - 1 **Project Management skills** are key in being able to deliver on engineered solutions, understand requirements and translate them into an IT or Cyber system for use
 - 2 **Organizational skills** play an important part of being able to demonstrate your ability to plan and execute
 - 3 Individuals that develop **collaborative** partnerships with other teams/departments are able to get more done