Security+ and Security Job Searching

Cybersecurity

Prep Week Day 2

Class Objectives

By the end of class, you will be able to:

- Understand how each domain is divided across the Security+ exam
- Prepare for Security+ questions from domains and topics that we have not explored in our curriculum, such as “Architecture and Design” and “Identity and Access Management.”
- Correctly answer Security+ practice questions.
- Identify a cyber career field that you are interested in and map out a career path toward a desired role.
- Begin developing your professional network.


WELCOME

Review

Last class, we learned that:

Certifications are broken into three types:

- Beginner certifications
- Advanced certifications
- Specialized certifications

Information security professionals take different certification paths depending on their interests.

One of the most popular beginner certifications is Security+.

One of the best methods to prepare for the Security+ exam is the CertMaster Practice tool, which you have access to through this course.

Today's Class

First half

We'll focus on several Security+ domains and the types of questions they contain.

Second Half

We'll explore cybersecurity career paths as well as networking and job searching strategies.

Security+ Domains

Security+ Exam Topics Breakdown

Security+ domain distribution:

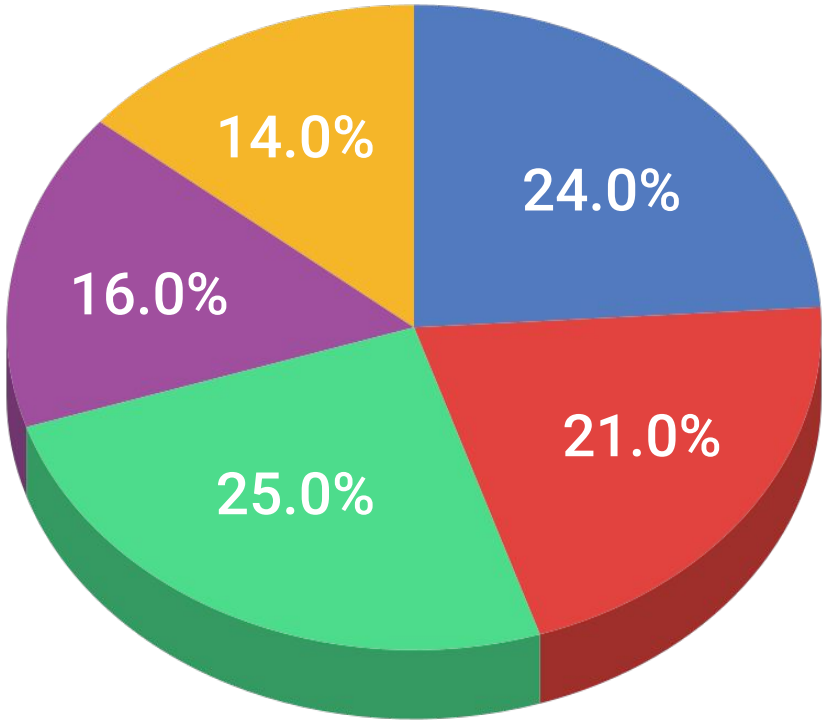
01 Attacks, Threats, and Vulnerabilities

02 Architecture and Design

03 Implementation

04 Operations and Incident Response

05 Governance, Risk, and Compliance



Today, we'll explore some subdomains that are outside the scope of this class—specifically, Identity and Access Management and Architecture and Design.

Identity & Access Management (IAM)

Identity and Access Management (IAM) refers to the security policies that ensure an organization's resources are only accessible by the right people, for the right reasons, at the right times.

There are significant risks to incorrectly assigning access to resources.


For example,
if an organization gives
all staff access to payroll
databases, they would be able
to view PII and other private
data of the organization
and its employees.

Identity and Access Management

Across the Security+ domains, several subdomains contain questions covering IAM, including:

2.4

Summarize authentication and authorization design concepts.

3.8

Given a scenario, implement authentication and authorization solutions.

Subdomain 2.4 Summarize authentication and authorization design concepts.

This subdomain focuses on the basic terms and concepts associated with IAM, such as **Authentication, Authorization, and Accounting (AAA)**: the framework to best control access to an organization's resources.

Types of authentication factors:

Something you are.
This includes biometrics, such as retina scanning or facial recognition.

Something you have.
Such as tokens or key cards.

Something you know.
Such as PINs and passwords.

Example Question:

Of the following authentication factors, which one is a different factor than a retina scan?

A. Hand geometry recognition

B. Voice recognition

C. Fingerprint recognition

D. Proximity cards

Example Question:

Of the following authentication factors, which one is a different factor than a retina scan?

A. Hand geometry recognition

B. Voice recognition

C. Fingerprint recognition

D. Proximity cards

Proximity cards are “something you have,” while the other options are all biometric factors (“something you are”).

Subdomain 3.8 Given a scenario, implement authentication and authorization solutions.

This subdomain focuses on the the application of the concepts associated with IAM, such as authentication protocols like:

Kerberos	An authentication protocol developed at MIT that uses tickets.
Password Authentication Protocol (PAP)	Uses a standard username and password to authenticate to a remote system. It is considered insecure.
Challenge-Handshake Authentication Protocol (CHAP)	Uses a three-way handshake, making it more secure than PAP.

Example Question:

Which of the following authentication protocols is considered insecure due to its lack of encryption?

A. EAP

B. SAP

C. PAP

D. CHAP

Example Question:

Which of the following authentication protocols is considered insecure due to its lack of encryption?

A. EAP

B. SAP

C. PAP

D. CHAP

PAP is insecure and unencrypted.

Subdomain 3.8 Given a scenario, implement authentication and authorization solutions.

This subdomain also focuses on the management decisions that make sure the right people have access to the right resources for the right reasons.

Types of access controls include:

- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Role Based Access Control (RBAC)

Subdomain 3.8

Given a scenario, implement authentication and authorization solutions.

This topic also focuses on selecting the optimal access controls based on your organization's environment.

For example:

Voice recognition is an appropriate biometric control if your office environment is relatively quiet.

Example Question:

Which of the following biometric controls would you select for a noisy office with good lighting that needed a cost-efficient solution?

A. Voice recognition

B. DNA analysis

C. Fingerprint recognition

D. Speech recognition

Example Question:

Which of the following biometric controls would you select for a noisy office with good lighting that needed a cost-efficient solution?

A. Voice recognition

B. DNA analysis

C. Fingerprint recognition

D. Speech recognition

A and D would not be optimal in a noisy office, and B would likely be an expensive biometric solution.

Subdomain 3.8 Given a scenario, implement authentication and authorization solutions.

This subdomain also focuses on how user accounts are managed, including the concept of least privilege: an individual or system should be given the minimum access rights needed to complete their tasks.

Account types:

User accounts	The basic, standard account type of users at your organization. These accounts are usually limited in privileges.
Guest accounts	Allow non-employees to have limited access to your organization's resources.
Privileged accounts	Have greater access than user accounts and are provided to managers and system administrators.

Example Question:

An external auditor needs limited access to your organization. What type of account should you provide them?

A. Guest account

B. User account

C. Sudo account

D. Service account

Example Question:

An external auditor needs limited access to your organization. What type of account should you provide them?

A. Guest account

B. User account

C. Sudo account

D. Service account

You would provide a guest account to a non-employee who needs limited access.

Activity: Security+ Identity and Access Management

In this activity, you will complete a quiz of performance-based and multiple-choice questions on Identity and Access Management topics.

Suggested Time:

15 Minutes

Time's Up! Let's Review.

Questions?

Security+ Architecture and Design Domain

Architecture and Design covers the processes and controls used to protect the confidentiality, integrity, and availability of an organization's data.

Architecture and Design

Within the Architecture and Design domain are eight subdomains:

01 Explain the importance of security concepts in an enterprise environment.

02 Summarize virtualization and cloud computing concepts.

03 Summarize secure application development, deployment, and automation concepts.

04 Summarize authentication and authorization design concepts.

05 Given a scenario, implement cybersecurity resilience.

06 Explain the security implications of embedded and specialized systems.

07 Explain the importance of physical security controls.

08 Summarize the basics of cryptographic concepts.

Architecture and Design

Today we'll focus on the three subdomains that have not been covered in our course:

01 Explain the importance of security concepts in an enterprise environment.

02 Summarize virtualization and cloud computing concepts.

03 Summarize secure application development, deployment, and automation concepts.

04 Summarize authentication and authorization design concepts.

05 Given a scenario, implement cybersecurity resilience.

06 Explain the security implications of embedded and specialized systems.

07 Explain the importance of physical security controls.

08 Summarize the basics of cryptographic concepts.

Subdomain 3 Summarize secure application development, deployment, and automation concepts.

This subdomain focuses on the concepts and processes relevant to developing secure applications for organizations and their users.

Input Validation

Restricts what data can be input to application fields, such as limiting non-ASCII characters.

Software development methodologies

Agile: A flexible development method that allows changes to the development requirements.

Waterfall: A structured and rigid development method where each step of the development cycle depends on the previous steps.

Example Question:

What is the biggest risk of outputting detailed application errors with coding details?

A. There is no risk, and it is recommended.

B. Coding details could provide the developer's name.

C. Coding details could illustrate vulnerabilities in the application code, which a hacker could then exploit.

D. Coding details could indicate when the code was written.

Example Question:

What is the biggest risk of outputting detailed application errors with coding details?

A. There is no risk, and it is recommended.

B. Coding details could provide the developer's name.

C. Coding details could illustrate vulnerabilities in the application code, which a hacker could then exploit.

D. Coding details could indicate when the code was written.

Displaying the code details, such as the coding language, version, and structure, could provide vulnerability information to hackers to exploit.

Subdomain 6 Explain the security implications of embedded and specialized systems.

This subdomain focuses on the security of systems that have hardware with software embedded within them.

A smart refrigerator:

- Is an example of an embedded system.
- Has software embedded within its hardware to complete specific tasks, such as monitoring temperature and determining if a filter needs replacing.

Architecture and Design

Terms to know include:

Supervisory Control and Data Acquisition (SCADA)

A system used to control technical equipment in industries such as:

- Energy
- Oil
- Water management

Internet of Things (IoT)

The network of devices that are connected to the internet, which are considered an extension of the internet itself. These devices include:

- Smart light bulbs
- Refrigerators
- Printers
- Door locks

Internet of Things (IoT)

is an expansive term relevant to many areas, such as smart houses, research and monitoring in the healthcare industry, wearable devices such as step counters, data collection in agriculture, manufacturing, city management, and many, many more.

Example Question:

To protect their data, which type of systems are usually not connected to the internet?

A. Linux servers

B. Apache web servers

C. SCADA systems

D. Home office networks

Example Question:

To protect their data, which type of systems are usually not connected to the internet?

A. Linux servers

B. Apache web servers

C. SCADA systems

D. Home office networks

While some SCADA systems have limited connection to the internet, they are usually not connected because they run high-impact systems.

Subdomain 7 Explain the importance of physical security controls.

This subdomain focuses on concepts associated with physical security processes and controls.

Environmental controls

For example:

- HVAC systems
- Fire suppression systems

Physical access controls

For example:

- Mantraps
- Security guards

Physical control types

For example:

- Deterrents, such as alarms
- Preventions, such as locks or gates

Example Question:

What type of risk can a bollard protect against?

A. Fire

B. Flooding

C. Vehicle access

D. Script kiddies

Example Question:

What type of risk can a bollard protect against?

A. Fire

B. Flooding

C. Vehicle access

D. Script kiddies

A bollard is a short post that's built into the ground to protect areas from vehicle access.

Activity: Security+ Architecture and Design Quiz

In this activity, you will take a quiz containing PBQ and multiple-choice questions from the Architecture and Design domain.

Suggested Time:

15 Minutes

Time's Up! Let's Review.

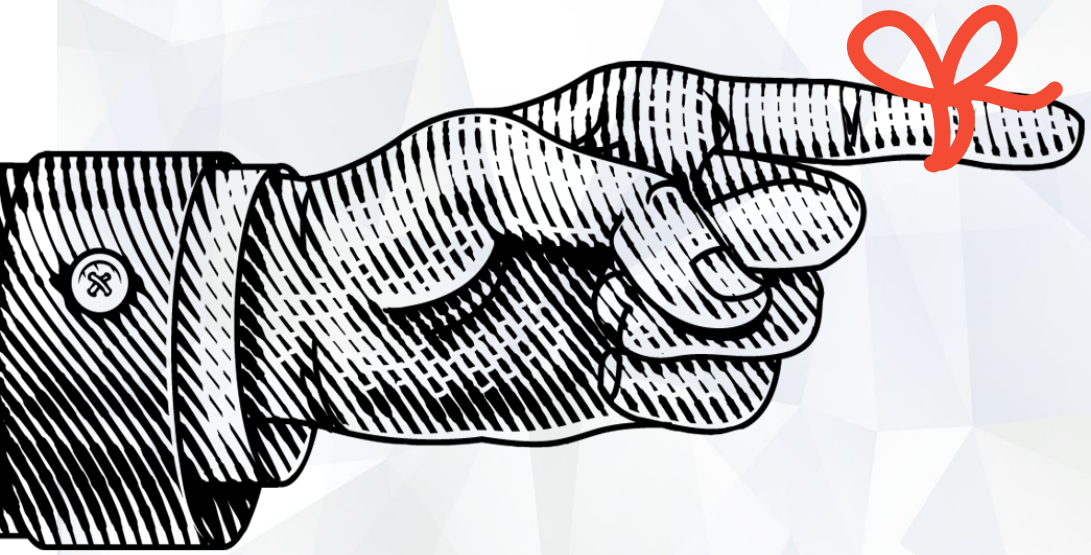
Questions?

Countdown timer

15:00

(with alarm)

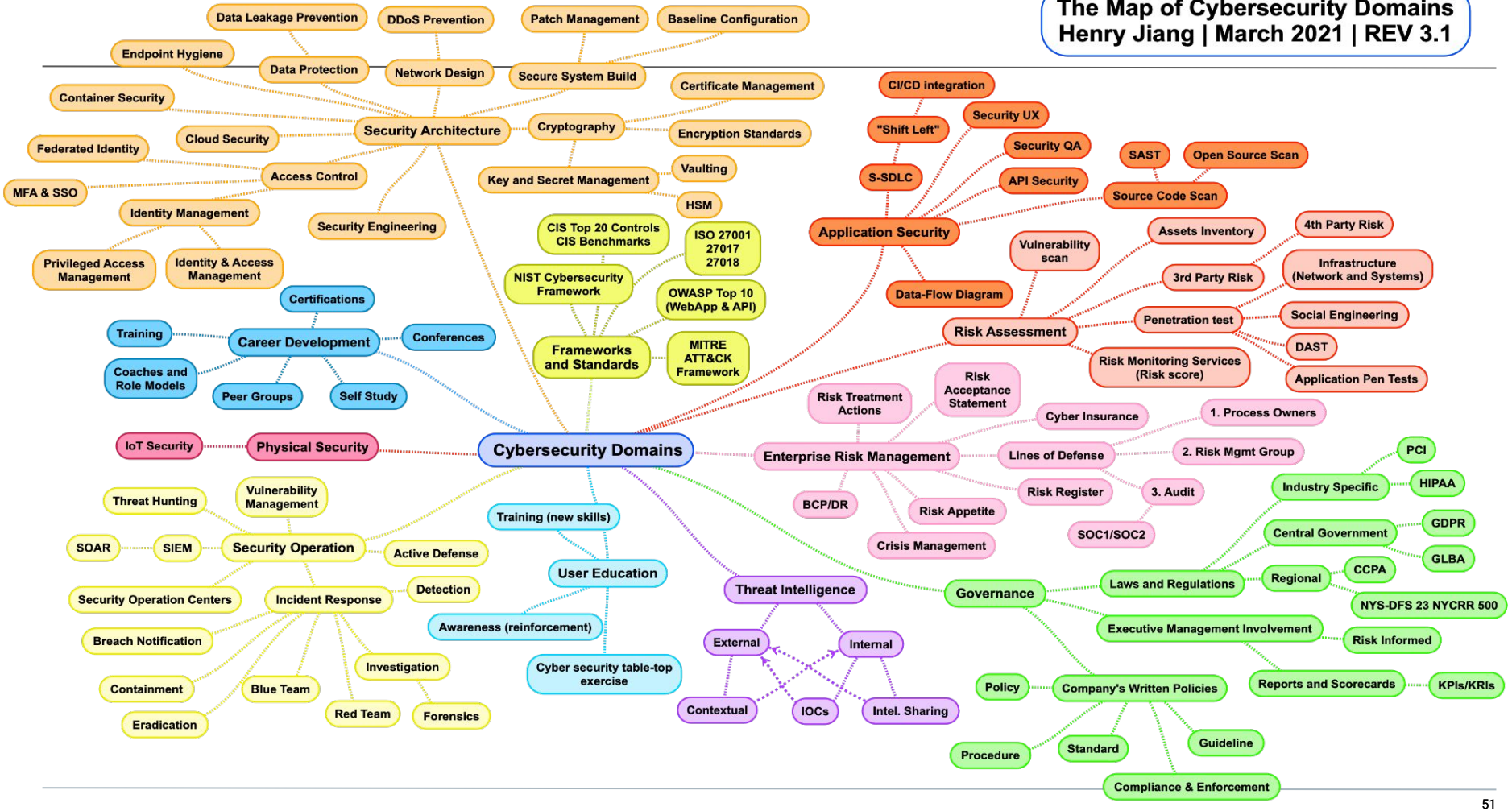
Cyber Career Paths



Remember,

In the very first week of class, we introduced the vast number of domains and specialties that exist in the cybersecurity industry.

The Map of Cybersecurity Domains
Henry Jiang | March 2021 | REV 3.1



Cybersecurity Domains

Security Architecture

Security design that addresses the requirements and potential risks of a given scenario or environment. It also specifies when and where to apply security controls.

Security Operation

Process of identifying, containing, and remediating threats on behalf of a company or organization.

Governance

Framework for managing performance and risk, oversight of compliance and control responsibilities, and defining the cyber mission by mapping the structure, authority, and processes to create an effective program.

Physical Security

Protection of personnel, hardware, software, networks, and data from physical actions and events that could cause serious loss or damage. Includes protection from fire, flood, natural disasters, burglary, theft, vandalism, and terrorism.

Threat Intelligence

Research and analysis of evidence-based knowledge regarding an existing or emerging menace.

Career Development

Training of future cybersecurity professionals.

Risk Assessment

Analyzing what can go wrong, how likely it is to happen, what the potential consequences are, and how tolerable the identified risk is.

User Education

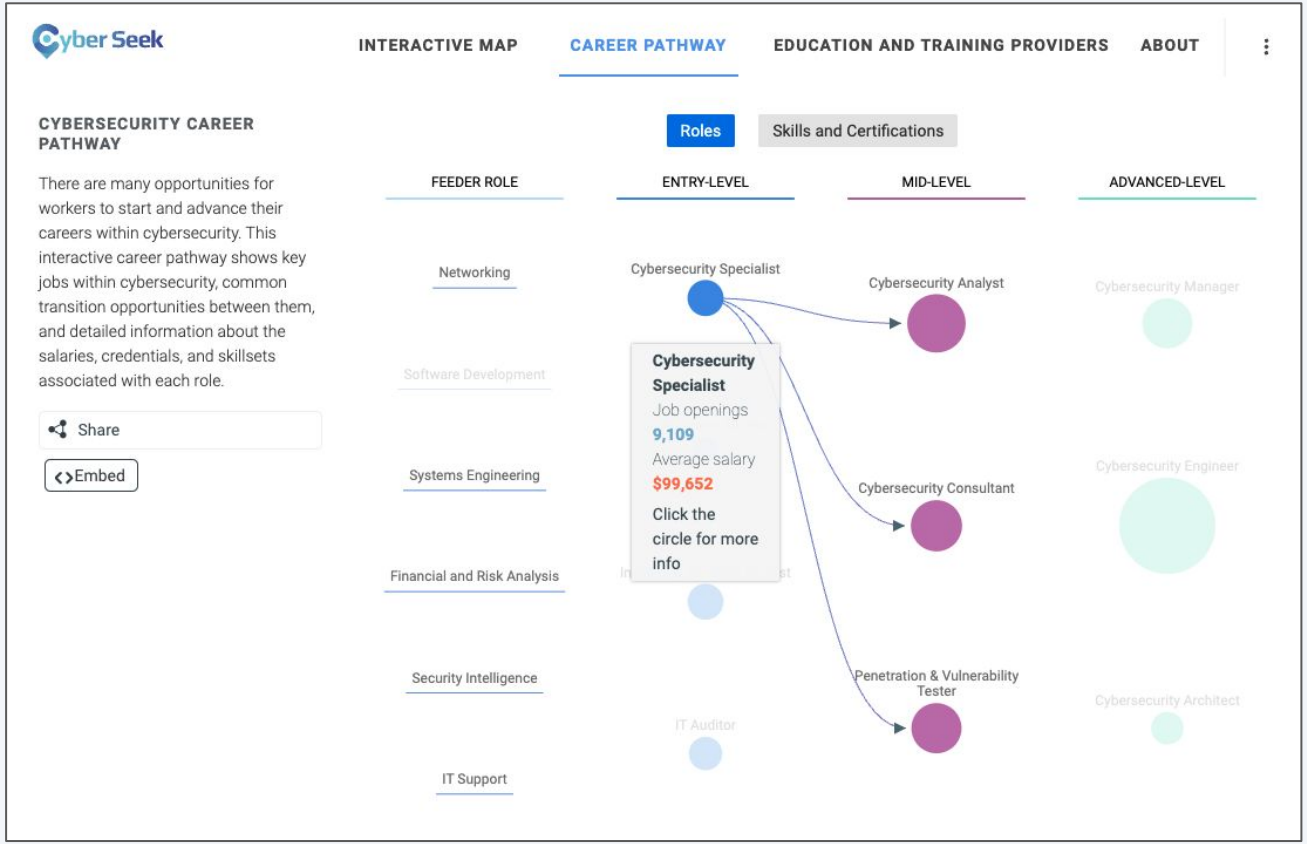
Teaching users how to protect themselves from cyberattacks by informing them of risks, exploits, and external threats, and the skills needed to combat common attacks.

Framework and Standard

Creation of new security frameworks and practices for professionals to follow.

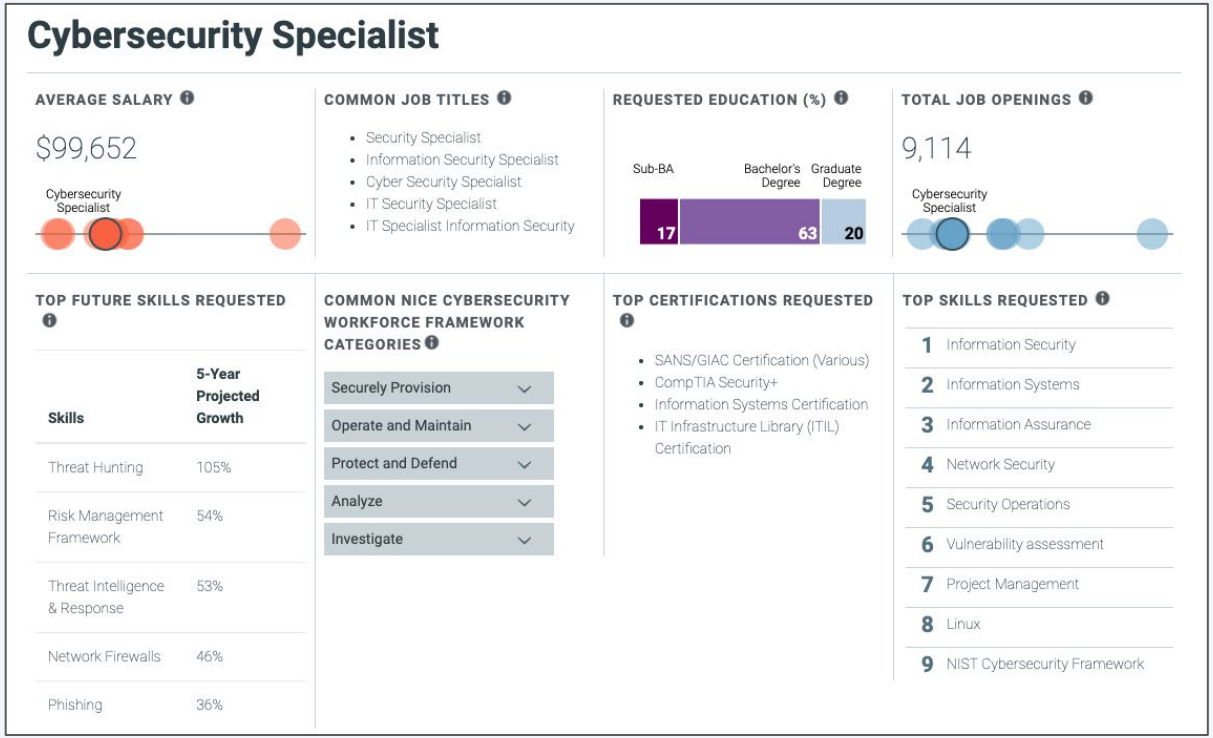
Cyber Career Pathways

The Cyberseek website is a great tool for exploring common career paths.



Cyber Career Pathways

Clicking on any of the featured roles will display helpful information, such as number of job openings, average salaries, desired skills and certifications



LinkedIn

Like a resume, a LinkedIn profile is a platform for demonstrating work history, skills, certifications, and achievements.

LinkedIn also allows you to build your network and to see real professionals' career pathways and development.

Activity: Career Paths

In this activity, you will use LinkedIn to research the career paths of several fellow cybersecurity professionals.

Suggested Time:

15 Minutes

Time's Up! Let's Review.

Questions?

Cyber Networking

While growing each year, the cybersecurity community is still a tight-knit, highly connected group of professionals.

Cyber Networking

Establishing connections and building your network can help in the following ways:

01

Through connections, you can meet other industry professionals, many of whom are actively hiring.

Hiring managers often circumvent the traditional job posting process and hire from personal recommendations.

02

Networking can provide resources for specific cyber domains.

For example, if you need to find a mobile forensic specialist and have a large network, it's likely that your network contains the specialist you need.

03

Connecting with professionals who are associated with trusted third-party companies and vendors can give you access to better pricing and personalized service.

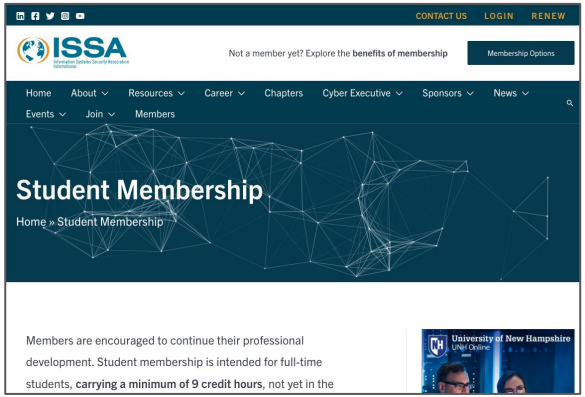
For example, a contact who works for a SIEM vendor could come in handy if you are looking for SIEM products for your organization.

By joining this course, you have already formed a cyber network consisting of everyone else here.

If you haven’t already, connect with one another on LinkedIn.

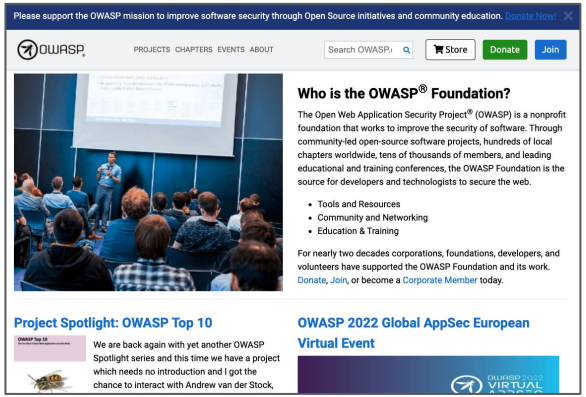
Cyber Groups, Chapters, and Organizations

The best way to build your network is to join local cyber groups, chapters, and professional associations.



https://www.issa.org

https://www.cyberstudents.org/



https://owasp.org/

Many of these have members who are also very new to the industry.

Cyber Groups, Chapters, and Organizations

The benefits of joining local cyber groups include:

- Regional specificity
- Welcoming attitude towards new professionals
- Monthly meetings, trainings, and social events
- Inexpensive or free membership and event cost

Specialized Cyber Groups

While many groups are offered for general cyber networking, there are also groups with specialized focuses.

Groups that emphasize certain technologies, such as cloud security groups like Cloud Security Alliance (CSA).

Groups that focus on specific industries, such as banking and finance security groups like Financial Services Information Sharing and Analysis Center (FSISAC).

Groups that connect people from specific demographics, such as the Women in Cyber Security (WiCyS).

Activity: Building Your Cyber Network

In this activity, you will start building your cyber network by researching cybersecurity groups and chapters local to your area.

Suggested Time:

15 Minutes

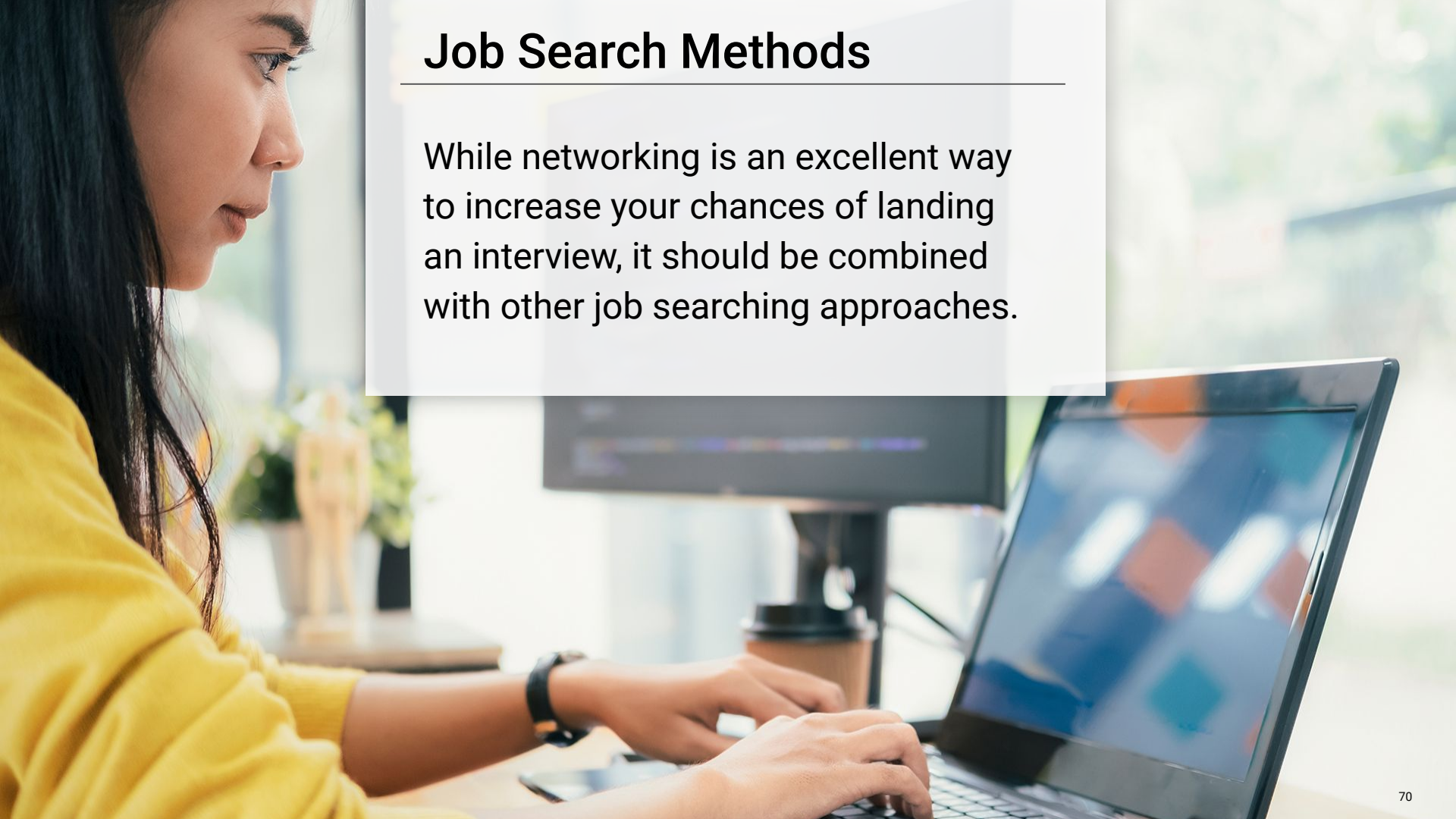
Time's Up! Let's Review.

Questions?

Job Searching Methods

Job Search Methods

While networking is an excellent way to increase your chances of landing an interview, it should be combined with other job searching approaches.



Traditional Job Search Methods

Traditional job search methods include:

01 Searching websites like Indeed, Dice, and Monster.com.

02 Searching for open positions on LinkedIn.

03 Working with a recruiter.

Traditional Job Search Methods

These methods are popular because of their comparatively easy application process and the clarity of details in job postings.

But, this same simplicity and clarity means you are often one of hundreds or thousands of applicants.

Cybersecurity professionals often use their creative thinking skills to “hack” the traditional approaches to job searching.

Non-Traditional Job Search Methods

Propose that an employer create a position for your skills.

- Share your observations of the organization's challenges or areas of need, and how your skills can address them.
- This is most successful at organizations where you have a personal connection.
- You could even do this at the organization where you currently work.

Non-Traditional Job Search Methods

Share your skills on platforms beyond LinkedIn and your resume.

Create blogs, custom websites, and videos to advertise your skills and find potential employers.

Attend cyber events where the primary purpose of the event is not job searching.

Increase your odds by attending cyber trade shows and conferences where you are one of fewer individuals looking for open positions.

Non-Traditional Job Search Methods

Reach out directly to the real decision maker at an organization.

We'll discuss this more in a moment.

Have you used, or can you think of, any other non-traditional job search methods?

Contacting Team Managers and Decision Makers

Recruiters and talent acquisition staff often manage the hiring process. But hiring decisions are typically made by managers and cybersecurity department leaders.

NOTE

This is a soft first introduction and does not mention open positions. That can be discussed in future meetings.

Jane Doe

123 Anywhere Ave, Everywhereville MN 00101 | 123-456-7890 | jdoe@2u.com

Hello,

I'm an aspiring cybersecurity professional transitioning from a career in {previous career}. As I make this transition, I am mapping out my job aspirations and pathways. I came across your profile and wanted to reach out to you because of your {success in X field/other reason}.

I {recently graduated/am about to graduate} from the cybersecurity boot camp at {school}, where I studied offensive and defensive security, web application security, and governance and compliance. I am also currently working on some exciting new projects, including {one-line project description}.

If you have a few minutes, I would love to pick your brain about how you got started, what you do at {company}, and how you maintain your expertise. Let me know if you're available for a quick coffee or phone/Zoom call sometime.

I look forward to hearing from you and appreciate your time either way!

Activity: Hacking Your Job Search

In this activity, you will “hack” your job search by applying non-traditional job search methods.

Suggested Time:

10 Minutes

Time's Up! Let's Review.

Questions?

Next Class

We'll focus on mock interviews and preparing for the interview process.


The End