EPNC CAREER COUNSELORS AND
ACADEMIC ADVISORS

CYBERSECURITY CAREERS TOOLKIT

Unlocking Cyber Success: Your Guide to Thriving in Security Careers.

TABLE OF

CONTENTS

PART I

INTRODUCTION TO CYBERSECURITY CAREERS

What is Cybersecurity?

Cybersecurity is the art of protecting information, information systems, networks, devices, and data from unauthorized access.

Cybersecurity professionals are like the digital world's police force, safeguarding our virtual valuables. Cybersecurity professionals are also responsible for protecting and maintaining secure and reliable communication (e.g., email, smartphones, tablets).

Imagine how much we depend on technology: from our personal devices like phones and laptops to massive online systems in fields such as farming, entertainment, shopping, and even banking. Cybersecurity experts are the guardians of this realm. They make sure that private conversations stay private, that our online shopping is safe, and that the systems we rely on every day are up and running without a hitch. They work in all sorts of industries, ensuring that everything from your favorite video game to the GPS in your car is secure.

Think about how often you use technology each day. Now, consider how important it is to have experts dedicated to protecting all that information you trust to the digital world. Whether it's personal data on your own devices or information stored across the internet, cybersecurity pros keep it under lock and key, just like security guards and police do in our physical world.

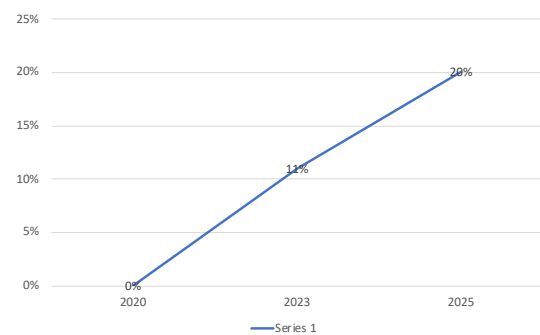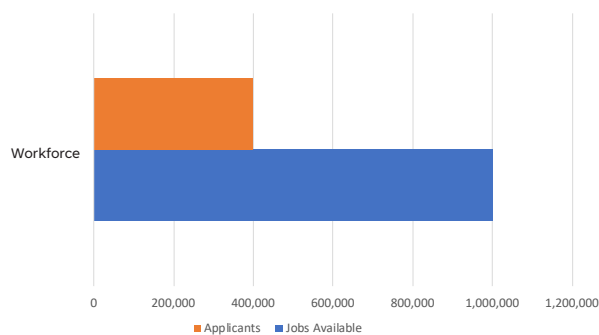## CYBERSECURITY
PRINCIPLES

Cybersecurity professionals are responsible for ensuring confidentiality, integrity, and availability of systems and information.

Cybersecurity professionals are employed across every sector of the economy including agriculture, manufacturing, education, entertainment (e.g., interactive video games, social media, apps), transportation (e.g., navigation systems), retail (e.g., online shopping, credit cards), medicine (e.g., medical equipment, medical records), logistics and supply chain, banking/financial industries, government services and the list goes on. How much of your daily life relies on technology?

DEFINING AND UNDERSTANDING THE
CYBERSECURITY WORKFORCE

The cybersecurity occupation is still a relatively new profession. However, this profession has grown exponentially over the last 20 years.

More than one million cybersecurity jobs will be available by 2023, but less than 400,000 cybersecurity professionals will be trained by then. Cybersecurity is an ever-growing industry. It is projected to grow by 11% in 2023 and by 20% in 2025. This is a fast-paced career with a median salary of $81,000.

The shortage of qualified professionals is largely due to the rapidly growth for new professionals as well as the growing cyber threats. By prioritizing and promoting cybersecurity careers, career and academic advisors help the nation and the local communities mitigate the risk of data breaches, financial losses, and interruptions to critical business operations and supply chains.

https://www.youtube.com/watch?v=wV2jmIS3oNE

CYBERSECURITY WORKFORCE
NICE FRAMEWORK

As the nation focuses on growing the cybersecurity workforce, a framework was needed to clarify the type of work and skills cybersecurity professionals need.

The *National Initiative for Cybersecurity Education* (*NICE) Workforce Framework* is the foundation for increasing the size and capability of the U.S. cybersecurity workforce. It provides a common definition of cybersecurity, a comprehensive list of cybersecurity work roles, the task performed by individual work roles and the knowledge, skills, and abilities required to perform those tasks. ([NICE Framework](#))

The Workforce Framework for Cybersecurity, commonly referred to as the NICE Framework, is a nationally focused resource to help employers develop their cybersecurity workforce.

It establishes a common lexicon that describes cybersecurity work and workers regardless of where or for whom the work is performed. The NICE Framework applies across public, private, and academic sectors. The NICE Framework is comprised of the following components:

7 CATEGORIES OF WORK

Oversight & Governance
Strategic planning and supervision of cybersecurity initiatives.

Design & Development
Creation and architecture of secure systems and applications.

Implementation & Operation
Deployment and maintenance of cybersecurity solutions.

Protection & Defense
Active defense against threats and vulnerabilities.

Investigation
Analysis and examination of cybersecurity incidents.

Cyberspace Intelligence
Gathering and analysis of cyber threat intelligence.

Cyberspace Effects
Actions taken to achieve objectives in cyberspace.

NICE FRAMEWORK STRUCTURE

- 7 Categories
- 11 Competency Areas
- 52 Work Roles
  - Tasks
  - Knowledge
  - Skills

NICE FRAMEWORK BREAKDOWN

7 Categories
A high-level grouping of common cybersecurity functions.

11 Competency Areas
Focus on capabilities in a particular domain.

52 Work Roles
The most detailed groupings of cybersecurity work comprised of specific knowledge, skills, and abilities (KSAs) required to perform tasks in a Work Role.

CYBERSECURITY CATEGORIES AND WORK ROLES

NICE FRAMEWORK

Category	Work Roles
OVERSIGHT AND GOVERNANCE (OG) - Provides leadership, management, direction, and advocacy so the organization may effectively manage cybersecurity-related risks to the enterprise and conduct cybersecurity work.	Communications Security (COMSEC) Management
	Cybersecurity Policy and Planning
	Cybersecurity Workforce Management
	Cybersecurity Curriculum Development
	Cybersecurity Instruction
	Cybersecurity Legal Advice
	Executive Cybersecurity Leadership
	Privacy Compliance
	Product Support Management
	Program Management
	Secure Project Management
	Security Control Assessment
	Systems Authorization
	Systems Security Management
	Technology Portfolio Management
	Technology Program Auditing
DESIGN AND DEVELOPMENT (DD) - Conducts research, conceptualizes, designs, develops, and tests secure technology systems, including on perimeter and cloud-based networks.	Cybersecurity Architecture
	Enterprise Architecture
	Secure Software Development
	Secure Systems Development
	Software Security Assessment
	Systems Requirements Planning
	Systems Testing and Evaluation
	Technology Research and Development
IMPLEMENTATION AND OPERATION (IO) - Provides implementation, administration, configuration, operation, and maintenance to ensure effective and efficient technology system performance and security.	Data Analysis
	Database Administration
	Knowledge Management
	Network Operations
	Systems Administration
	Systems Security Analysis
	Technical Support

Introduction to the
NICE Framework

CYBERSECURITY CATEGORIES AND WORK ROLES

NICE FRAMEWORK

Category	Work Roles
PROTECTION AND DEFENSE (PD) - Protects against, identifies, and analyzes risks to technology systems or networks. Includes investigation of cybersecurity events or crimes related to technology systems and networks.	Defensive Cybersecurity
	Digital Forensics
	Incident Response
	Infrastructure Support
	Insider Threat Analysis
	Threat Analysis
	Vulnerability Analysis
INVESTIGATION (IN) - Conducts national cybersecurity and cybercrime investigation, including the collection, management, and analysis of digital evidence.	Cybercrime Investigation
	Digital Evidence Analysis
CYBERSPACE INTELLIGENCE (CI) - Collects, processes, analyzes, and disseminates information from all sources of intelligence on foreign actors' cyberspace programs, intentions, capabilities, research and development, and operational activities.	All-Source Analysis
	All-Source Collection Management
	All-Source Collection Requirements Management
	Cyber Intelligence Planning
	Multi-Disciplined Language Analysis
CYBERSPACE EFFECTS (CE) - Plans, supports, and executes cyberspace capabilities where the primary purpose is to externally defend or conduct force projection in or through cyberspace.	Cyberspace Operations
	Cyber Operations Planning
	Exploitation Analysis
	Mission Assessment
	Partner Integration Planning
	Target Analysis
	Target Network Analysis

[Introduction to the NICE Framework](#)

The NICE Framework has at its foundation Task, Knowledge, and Skill (TKS) statements, which are then used to form Work Roles and Competency Areas:

- **Task Statement:** Description of a work activity directed towards the achievement of organizational objectives.
- **Knowledge Statement:** Description of a retrievable set of concepts in a learner's memory.
- **Skill Statements:** Description of a learner's capacity to perform an observable action.
- **Work Roles:** Groupings of work for which an individual or team is responsible or accountable. Work Roles are organized into high-level Work Role Categories and are composed of Tasks that constitute work to be done.
  Competency Areas: Clusters of related Knowledge and Skill statements that correlate with one's capability to perform Tasks in a particular domain.

CYBERSECURITY
CAREER PROFILES

Another way to understand the cybersecurity workforce involves analyzing various career profiles.

The cybersecurity profession typically refers to individuals tasked with safeguarding information and information systems. The NICE Framework demonstrates that protecting these systems requires a diverse range of professionals, which reflects the variety of systems in need of protection. Virtually every segment of our economy faces the threat of cyber-attacks, including sectors such as government, education, banking, financial services, healthcare, manufacturing, retail sales, insurance, transportation, energy, national defense, and even education itself.

The array of cybersecurity professionals is vast, encompassing roles such as technicians, engineers, programmers, scientists, architects, auditors, administrators, executives, investigators, intelligence officers, legal experts, and educators. Given this diversity, it can be challenging for educators, career counselors, and advisors to assist students in identifying and planning a path to a suitable cybersecurity career. However, numerous organizations offer resources to support educators in promoting cybersecurity careers.

Using CYBER.ORG Online Tools

CYBER.ORG - is a cybersecurity workforce development organization that targets K-12 students with cyber career awareness, curricular resources, and teacher professional development. One of the many valuable products produced by this organization are their "Cyber Career profiles" see (Figure 4) These posters can be download from https://cyber.org/career-exploration/cyber-career-profiles.

The website has a wealth of additional cybersecurity resources for educators, students, and parents. Have your students select one of the career profiles. Have student identify the type of information provided within the career profile. Compare the difference between this tool and the NICE Framework data.

You can also explore cybersecurity careers with 14 virtualized challenges at **trycyber.us**

CYBERSEEK WEBSITE

CAREER PATHWAYS
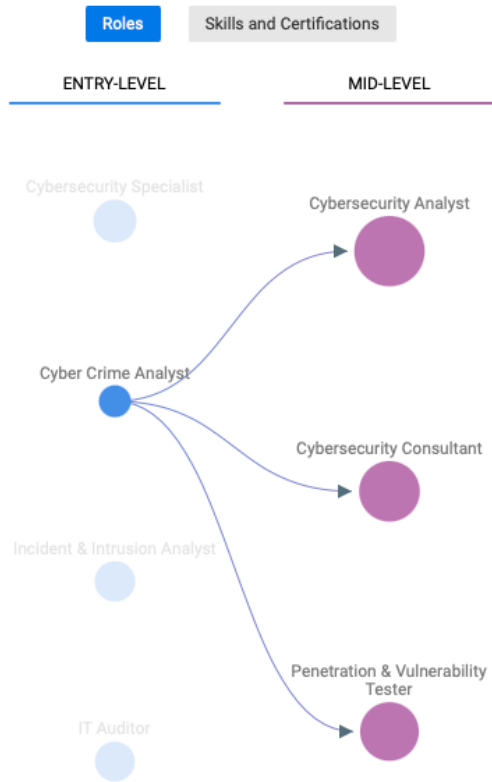
Cyberseek is a joint initiative between the National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce and Lightcast, a leading provider of job market analytics and strategic intelligence.

The *CyberSeek Pathway* tool was demonstrated as a mechanism to identify entry-, mid-, and advanced-level cybersecurity jobs and apply the NICE Cybersecurity Workforce Framework to help individuals identify the knowledge, skills, and abilities necessary for career advancement.

CyberSeek can support local employers, educators, guidance and career counselors, students, current workers, policy makers, and other stakeholders as they answer various questions about the cybersecurity workforce.

https://www.cyberseek.org/pathway.html

Explore

Have your student lookup the following jobs roles:

- Cybersecurity Specialist
- IT Auditor
- Cyber Crime Analyst
- Cybersecurity Manager

Explore Here!

CYBERSEEK WEBSITE

INTERACTIVE HEAT MAP

Have students use the Interactive Cybersecurity Career Map to explore jobs in their states and metropolitan areas.

Prompt them to find the following information:

- Total job openings
- Supply/demand ratio
- Top jobs in the area
- Jobs in each of the seven NICE categories
- Credentials

https://www.cyberseek.org/heatmap.html

State/Metro Area	Total Cyber Job Openings	Top Job Titles	Second Job Title	Top NICE Category	CISSP Holders/ Openings	CISA Holders/ Openings
Illinois						
Chicago						
Virginia						
Los Angeles						
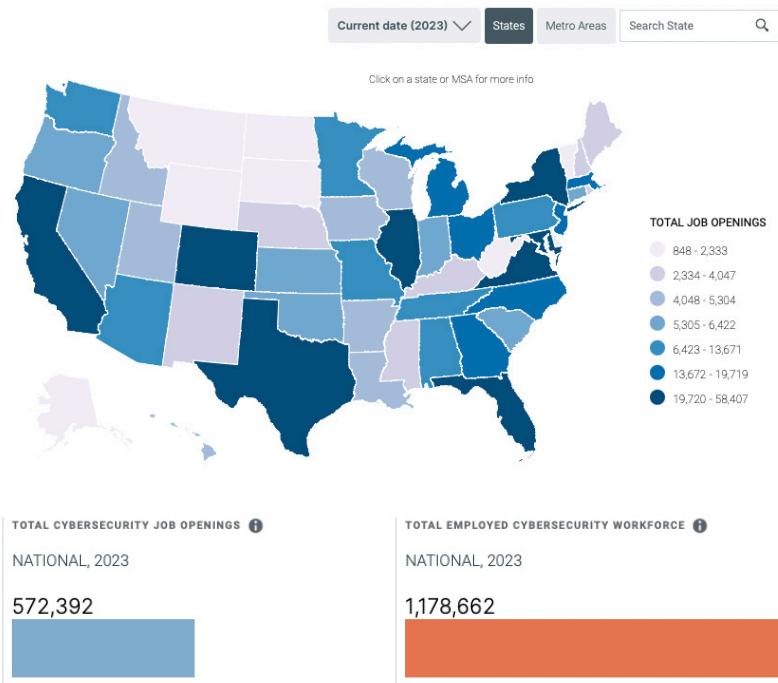
🔍 Explore Use the Interactive Cybersecurity Career Map to complete the table below:

PART II

WHY STUDENTS SHOULD CONSIDER A CAREER IN CYBERSECURITY

WHY CONSIDER A
CAREER IN CYBERSECURITY?

OPPORTUNITIES ABOUND

Cybersecurity faces a shortage of skilled professionals, expected to persist, leading to abundant job opportunities, above-average pay, and a secure career path for students.

REWARDING COMPENSATION

Due to the high demand and the specialized skill set required, careers in cybersecurity offer excellent salaries and benefits. Professionals in this field often receive compensation well above the average, making it an economically appealing choice.

DIVERSE NATURE OF WORK

Cybersecurity offers dynamic and non-monotonous work, demanding critical thinking, teamwork, and continual learning. The evolving threat landscape requires constant adaptation, making it ideal for individuals who thrive on challenges and innovation.

SERVICE TO OTHERS

A career in cybersecurity goes beyond personal gain; it's about service. Professionals safeguard data and infrastructure, contributing to national security and the well-being of communities, families, and friends, ensuring the security of local businesses and vital services.

CAREER OPPORTUNITIES

Cybersecurity provides diverse roles in various industries, from frontline defense to data analysis, catering to different strengths and interests. There's a place in cybersecurity for every type of problem-solver.

SERVING NATIONAL INTERESTS

At the highest level, cybersecurity experts contribute to national security. They play a critical role in protecting a nation's secrets and infrastructure, making the work not only personally fulfilling but also patriotic.

In summary, a cybersecurity career offers students a chance to enter a field where they can constantly learn and grow, earn a generous income, and make a difference in the lives of others and the security of their country.

PART III

UNDERSTANDING ACADEMIC CREDENTIALS

PURPOSE OF
ACADEMIC CREDENTIALS

Academic credentials serve as evidence that a student completed education and/or training in a specific field, earn college credit and have developed necessary workforce competencies to qualify for entry-level employment.

Many colleges also group the certificates in college majors or minors. Majors are primary fields of study, and minors are secondary concentrations that may or may not be related to your major. Although the two can be similar, they do not need to be. Many students choose a minor later in their academic career. This minor can be based upon an area of interest that they discovered, or a way to complement their existing major and possibly make them more attractive in the workplace.

Academic Credentials
(College Degrees and Certificates)

There are five main categories of academic credentials, commonly known as academic certificates or degrees. College certificates have gained popularity over time, with more students opting to earn them. These short-term programs, requiring 12 to 60 college credits, focus on specific skills in demanding fields such as cybersecurity. Additionally, these certificates can be stackable, allowing individuals to start with basic skills certificates and progress to more technical or advanced certificates, ultimately leading to a full college degree.

Bachelor's Degree Programs

A bachelor's degree is a four-year program typically offered at universities and colleges, offering in-depth knowledge and specialization in various fields of study. Types of bachelor's degrees include *Bachelor of Arts (BA), Bachelor of Science (BS), Bachelor of Fine Arts (BFA), Bachelor of Applied Science (BAS), Bachelor of Business Administration (BBA), Bachelor of Engineering (BEng), and Bachelor of Computer Science (BCS)*.

These programs open up extensive career opportunities and serve as a foundation for advanced education, providing comprehensive knowledge and skills in fields such as business, technology, healthcare, and liberal arts. Graduates can choose to enter the workforce directly or pursue further education in graduate or professional programs.

PURPOSE OF

ACADEMIC CREDENTIALS

Admission Requirements for Bachelor's Degree Programs

Admission requirements for bachelor's degree programs vary among colleges and universities. However, common conditions for enrollment include:

- High school diploma or equivalent
- Meeting minimum GPA requirements
- SAT or ACT scores (depending on the institution)
- Submission of application forms and required documents

Average Cost of Bachelor's Degree Programs

The cost of a bachelor's degree program varies depending on the institution, program, and whether it is a public or private college. On average, the tuition for a four-year bachelor's degree program is significantly higher than that of an associate degree. In 2021, the average annual tuition for public in-state schools was $10,740, while public out-of-state schools averaged $27,560 (according to the College Board, 2020). It's important to note that these figures are subject to change, and tuition fees may increase over time.

Full-Time Versus Part-Time Students

Most students pursuing a bachelor's degree attend college on a full-time basis. Typically, it takes full-time students four years to complete their bachelor's degree, which usually consists of around 120 credits or 180 credits for schools on a quarter system. Full-time students usually take 4-5 classes per semester, although this may vary depending on the institution and program structure.

However, part-time attendance is also common among bachelor's degree students. Part-time students may take longer to complete their degree due to fewer courses taken per semester. This flexible option allows students to balance work or other responsibilities while pursuing their education. In 2021, more than 2.2 million students attended college full-time, while approximately 4 million students attended part-time. Many part-time students also work while studying, with 72 percent of them holding jobs while pursuing their degree.

Overall, bachelor's degree programs provide in-depth education and specialization in various fields, opening doors to a wide range of career opportunities. Admission requirements vary, and tuition costs are typically higher than those of associate degree programs. Students can choose between full-time and part-time enrollment based on their preferences and circumstances.

PURPOSE OF

ACADEMIC CREDENTIALS

Master's Degree Programs

A master's degree is an advanced level of education that follows the completion of a bachelor's degree. It provides in-depth knowledge, specialization, and advanced skills in a specific field of study. Master's degree programs are typically offered at universities and colleges and are available in various disciplines.

Types of Master's Degrees

- Master of Arts (MA)
- Master of Science (MS)
- Master of Business Administration (MBA)
- Master of Education (MEd)

- Master of Engineering (MEng)
- Master of Fine Arts (MFA)
- Master of Public Health (MPH)
- Master of Social Work (MSW)

Average Cost of Master's Degree Programs

Master's degree program costs vary based on the institution, program length, and field of study. Generally, tuition is higher than for bachelor's degrees, ranging from $10,000 to $40,000 per year. Financial aid options, like scholarships and grants, can help ease the financial burden. Some employers also provide tuition assistance for employees pursuing advanced degrees.

Full-Time Versus Part-Time Students

Master's degree programs can be pursued on a full-time or part-time basis, depending on the student's preference and availability. Full-time study typically involves dedicating oneself to the program on a full-time basis, often completing the degree in one to two years, depending on the program's structure. Part-time study allows students to balance their education with other commitments such as work or family responsibilities. Part-time programs may take longer to complete, typically extending the duration to two to four years.

The choice between full-time and part-time enrollment depends on individual circumstances, such as work obligations, financial considerations, and personal commitments.

In summary, master's degree programs offer advanced education, specialized knowledge, and skills in various fields. Admission requirements, tuition costs, and program duration vary among universities and disciplines. Whether pursued on a full-time or part-time basis, a master's degree provides graduates with enhanced career prospects, increased expertise, and the potential for leadership roles in their chosen field.

PURPOSE OF
ACADEMIC CREDENTIALS

Advanced Degrees: Doctoral Programs (PhD)

A doctoral degree, commonly known as a PhD (Doctor of Philosophy), is the highest level of education one can achieve in most fields of study. Doctoral programs are rigorous and research-focused, preparing students for advanced scholarly work and making significant contributions to their chosen field. Doctoral degrees are offered by universities and academic institutions worldwide.

Types of Advanced Degrees

- Doctor of Philosophy (PhD)
- Doctor of Business Administration (DBA)
- Doctor of Education (EdD)
- Doctor of Engineering (EngD)

Doctoral degrees provide extensive specialization, advanced research skills, and the ability to critically analyze and contribute to knowledge in a specific field. Doctoral students are typically required to complete original research, write a dissertation or thesis, and defend their work before a panel of experts. The completion of a PhD program demonstrates the highest level of expertise and scholarly achievement.

Average Cost of Doctoral Programs

The cost of doctoral programs can vary significantly depending on the university, program, and field of study. Generally, doctoral programs are funded, offering stipends, teaching or research assistantships, or fellowships to admitted students. These financial packages often cover tuition and provide a modest living allowance. In some cases, students may need to seek external funding or secure scholarships to support their studies.

Full-Time Versus Part-Time Students

Doctoral programs primarily require full-time commitment due to the intensity of the research and coursework involved. Students typically dedicate several years, ranging from three to seven or more, to complete their doctoral studies. The duration depends on factors such as the field of study, research requirements, and individual progress. While part-time doctoral programs exist, they are less common due to the extensive nature of doctoral research.

Doctoral degrees equip graduates with advanced knowledge, research expertise, critical thinking skills, and leadership capabilities in their respective fields. They open doors to academic positions, research careers, industry leadership roles, and influential positions in government or policy-making institutions. Pursuing a doctoral degree represents the pinnacle of intellectual achievement and fosters lifelong contributions to knowledge and innovation.

PART IV

CYBERSECURITY MAJORS

TYPES OR MAJORS OF ACADEMIC
CYBERSECURITY PROGRAMS

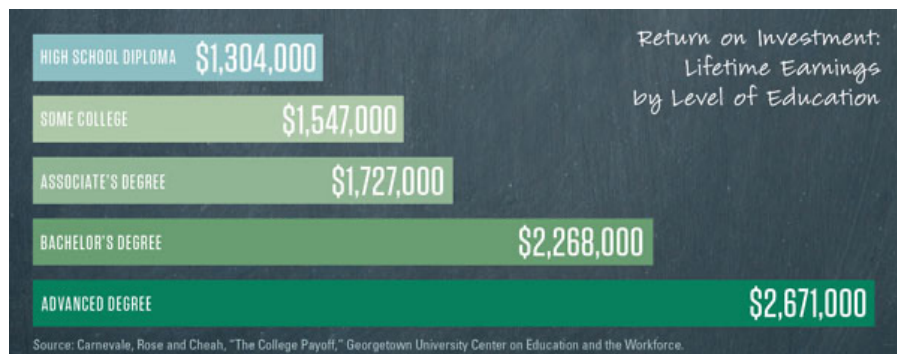| Major	Description	Example Career
Cyber Defense	Learn to protect computer systems and networks from cyber-attacks, identify threats, and create strategies for information security.	Cybersecurity Analyst
Cyber Operations	Focuses on offensive and defensive tactics in cybersecurity, learning techniques to detect, respond to, and prevent cyber threats.	Penetration Tester
Digital/Network Forensics	Learn to investigate cybercrimes, gather evidence from digital devices or networks, and analyze data for legal or security purposes.	Digital Forensic Analyst
Information System Security Management	Focuses on managing and securing information systems within organizations, including risk assessment, security policies, and incident response.	Security Manager
Governance, Auditing, Risk Management (GRC)	Involves managing risks, ensuring compliance with cybersecurity regulations, and evaluating security measures within organizations.	Cybersecurity Consultant
Legal/Compliance	Focuses on the legal aspects of cybersecurity, including privacy laws, regulations, and compliance requirements.	Cybersecurity Legal Consultant
Intelligence	Learn to gather and analyze information to identify and prevent cyber threats, with a focus on threat intelligence and cybersecurity analysis.	Cybersecurity Analyst in Government Agency
Artificial Intelligence	Explores the intersection of AI and cybersecurity, leveraging AI technologies to enhance cybersecurity defenses.	Cybersecurity AI Specialist
Data Science/Security	Focuses on using data analysis techniques to enhance cybersecurity, analyzing large amounts of data to identify patterns and potential security risks.	Cybersecurity Data Analyst

DEGREES AND LIFETIME
EARNING POTENTIAL

Having a college degree greatly improves your chances of finding a job and earning more money.

Individuals with a bachelor's degree face only half the likelihood of unemployment compared to those with only a high school diploma, and, on average, they accumulate an additional $1.2 million in lifetime earnings. A comprehensive study by economists, examining outcomes for over 30 million students, reveals that attending public universities offers the most promising economic advancement. Opting for a public university education can pave the way for a more prosperous financial future.

In essence, obtaining a college degree significantly impacts employment opportunities and income potential. It's crucial to weigh these advantages when making decisions about your education and future career.

Return on Investment: Lifetime Earnings by Level of Education

HIGH SCHOOL DIPLOMA	$1,304,000
SOME COLLEGE	$1,547,000
ASSOCIATE'S DEGREE	$1,727,000
BACHELOR'S DEGREE	$2,268,000
ADVANCED DEGREE	$2,671,000

Source: Carnevale, Rose and Cheah, "The College Payoff," Georgetown University Center on Education and the Workforce.

🔍 **Explore** Find at least four academic credentials related to cybersecurity that interest you. Record the information in the table below:

INSTITUTION	DEGREE	SUBJECT AREA	YEARS TO COMPLETE

PART V

CYBERSECURITY INDUSTRY CREDENTIALS

CYBERSECURITY

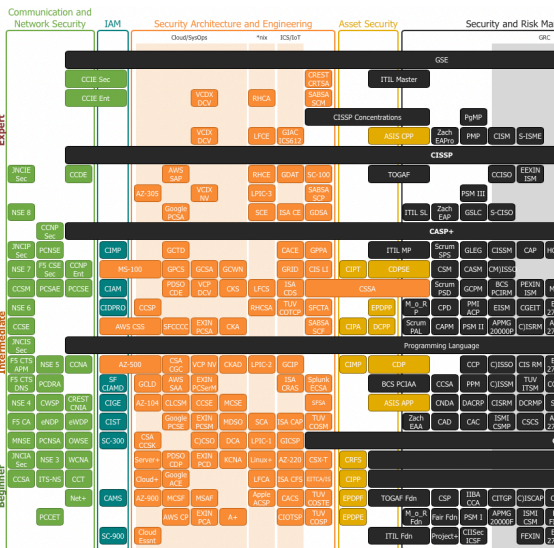# INDUSTRY CERTIFICATIONS

In the fast-paced world of cybersecurity, having the right education credentials is just the starting point.

[Certification Pyramid, Paul Jerimy](#)

What truly sets you apart are industry certifications—official stamps of approval that you earn by acing exams and racking up real-world experience. These certifications matter for a bunch of reasons. For newbies cutting their teeth in tech, they mark a universal baseline of your knowledge skills and use of certain tech tools. For the seasoned pros, they're a way to flaunt their prowess in specific tech domains. And from an organization's perspective, certifications are proof that they've got the best brains working to shield their digital assets in the case of data breaches or attacks.

Cybersecurity Industry Certification Organizations

When it comes to cybersecurity industry certification there's no shortage of organizations offer endorsements. Yet, some credentials carry more clout in the industry, getting you a nod of respect from the cybersecurity community and a thumbs-up from the individuals hiring new talent. But don't write off the underdogs; some gigs might specifically want you to have their lesser known, yet still shiny, certificates. The bottom line: if you're just diving in or you're after certs that'll open doors anywhere, aim for the top-tier ones from the big five in the biz.
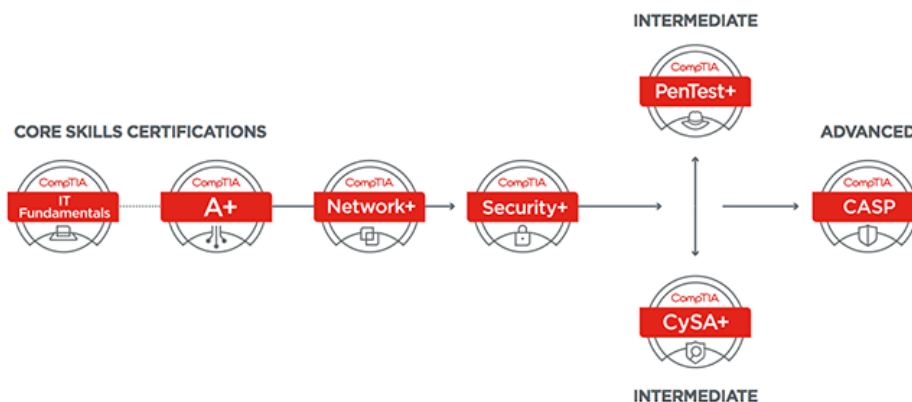
CYBERSECURITY

INDUSTRY CERTIFICATIONS

CompTIA – Computing Technology Industry Association

CompTIA certifications are some of the most highly recognized IT certifications available. CompTIA provides certifications in many different IT fields such as software development, computer networking, cloud computing, and of course, information security. Though not all these certifications are security-specific, they form the bedrock for more specialized cybersecurity credentials offered by CompTIA. These higher-tier certifications include:

- **CASP+ (CompTIA Advanced Security Practitioner):** Tailored for experienced practitioners, this advanced certification equips security architects and senior security engineers with the skills to bolster enterprise cybersecurity.

- **CompTIA CySA+ (Cybersecurity Analyst):** A notch above Security+, this cert preps you for the role of a cybersecurity analyst, sitting just below the expertise required for CASP+.

- **CompTIA Security+:** The ideal launchpad for a cybersecurity career, covering key concepts in network security and risk assessment.

These certifications collectively aim to provide a structured and comprehensive career pathway for IT professionals aspiring to specialize in cybersecurity.
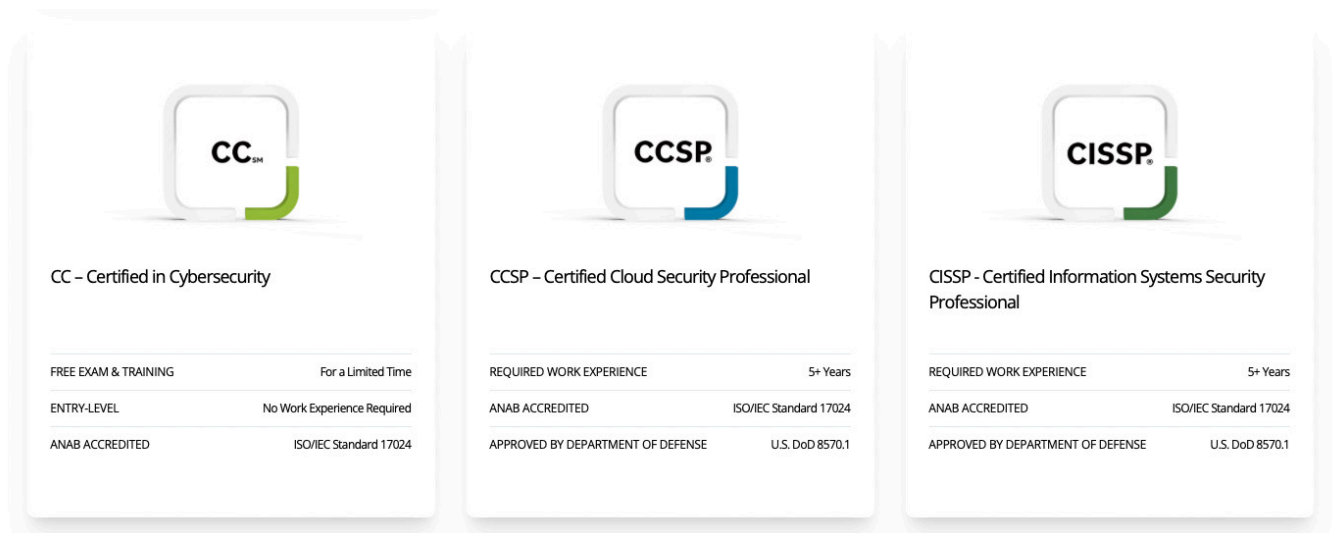
CYBERSECURITY

INDUSTRY CERTIFICATIONS

ISC2 - The International Information System Security Certification Consortium

The International Information Systems Security Certification Consortium, more commonly known as (ISC)2, is the organization behind the sought after CISSP certification. The (ISC)2 boasts itself on their website as "The World's Leading Cybersecurity Professional Organization". (ISC)2 is a non-profit with more than 140,000 certified members. (ISC)2 offer certifications such as:

- **CISSP (Certified Information Systems Security Professional):** is one of the most sought after and most esteemed certifications in the cybersecurity world. The CISSP should be on the list of anyone hoping to be successful in the industry.

- **SSCP (Systems Security Certified Practitioner):** is a great certification for professionals looking to bring growth to their careers.

CC – Certified in Cybersecurity		CCSP – Certified Cloud Security Professional		CISSP - Certified Information Systems Security Professional	
FREE EXAM & TRAINING	For a Limited Time	REQUIRED WORK EXPERIENCE	5+ Years	REQUIRED WORK EXPERIENCE	5+ Years
ENTRY-LEVEL	No Work Experience Required	ANAB ACCREDITED	ISO/IEC Standard 17024	ANAB ACCREDITED	ISO/IEC Standard 17024
ANAB ACCREDITED	ISO/IEC Standard 17024	APPROVED BY DEPARTMENT OF DEFENSE	U.S. DoD 8570.1	APPROVED BY DEPARTMENT OF DEFENSE	U.S. DoD 8570.1

CYBERSECURITY
INDUSTRY CERTIFICATIONS

EC-Council

Rather than focusing on specific areas of knowledge, EC-Council markets more towards specific roles and titles. For example, when a professional look at the certification programs on EC-Council's website, they would see that the certifications look more like job titles: Licensed Penetration Tester, Certified Ethical Hacker, Security Analyst, Certified Chief Information Security Officer, and the list goes on. This can make it easy for those interested in a specific job to focus on which certification they'd like to pursue. On the other hand, these certifications may be too specialized for individuals looking to cover a wide range of security skills. Some of the certifications provided by EC-Council are listed below:

- **CEH (Certified Ethical Hacker):** is the most well-known of the EC-Council certifications. The CEH is widely recognized among security professionals. While the certification may include the word hacker in its title, it's not just for those who work in offensive security.

- **CND (Certified Network Defender):** certification is appropriate for anyone who works in the network administration or cybersecurity fields in the capacity of a network administrator, network engineer, network security administrator, or security analyst. CND is for all cybersecurity operations and roles, and it is applicable for anyone looking to build a career in this domain.

CORE	CORE	SPECIALIZE	EXECUTIVE
C ND Certified Network Defender	**C EH** Certified Ethical Hacker	**C HFI** Computer Hacking Forensic INVESTIGATOR	**C CISO** Certified Chief Information Security Officer
IAT Level I	CSSP Analyst	CSSP Infrastructure Support	IAM Level II
IAT Level II	CSSP Infrastructure Support	CSSP Incident Responder	IAM Level III
IAM Level I	CSSP Incident Responder		CSSP Manager
CSSP Infrastructure Support	CSSP Auditor		

CYBERSECURITY
INDUSTRY CERTIFICATIONS

GIAC – SANs and Global Information Assurance Certification

The Global Information Assurance Certification is an organization founded in 1999 to validate the skills of information security professionals. GIAC certifications are trusted by thousands of companies and government agencies, including the United States National Security Agency (NSA). GIAC certifications are based on SANS training. GIAC offers many different certifications in categories such as cyber defense, penetration testing, incident response, and forensics as well as a few others. The GIAC certifications include:

- **GSEC (GIAC Security Essentials)** is an entry-level certification offered by GIAC. It certifies a practitioner's knowledge of information security that goes beyond simply knowing terminology and concepts. The goal of the GSEC is to validate an individual's hands-on knowledge.

- **GCFA (GIAC Certified Forensic Analyst)** is a widely recognized forensic analyst certification that covers a wide range of forensic topics such as advanced incident response and digital forensics, memory forensics, timeline analysis, anti-forensics detection, threat hunting, and APT intrusion incident response.

CYBERSECURITY

INDUSTRY CERTIFICATIONS

ISACA - Information Systems Audit and Control Association

Previously known as the Information Systems Audit and Control Association, ISACA now goes by its acronym only. According to their website, ISACA was incorporated in 1969 by a small group of individuals who recognized a need for a centralized source of information and guidance in the growing field of auditing controls for computer systems. Since then, thousands of IT professionals have gone on to obtain ISACA certifications such as:

- **CISA (Certified Information Systems Auditor)** certification is a widely recognized certification that covers information security audit control, assurance and security.

- **CISM (Certified Information Security Manager)** is a step above the CISA. This certification is designed for those who would like to demonstrate their knowledge of information security management.

CISA Certified Information Systems Auditor. An ISACA® Certification

CRISC Certified in Risk and Information Systems Control. An ISACA® Certification

CISM Certified Information Security Manager. An ISACA® Certification

CGEIT Certified in the Governance of Enterprise IT. An ISACA® Certification

🔍 **Explore**   Have your students research three other certification bodies. What entry level and expert level (highest level) certifications do they provide?

CERTIFICATION BODY	ENTRY LEVEL	EXPERT LEVEL

VALUE OF
CERTIFICATIONS

Certifications are worth the time and effort you put into them.

When you successfully complete a certification, it can lead to immediate promotions, better job opportunities, or even a raise in your current position. Surveys consistently show that earning a certification can result in a salary increase of up to 5%.

Distinction

There are several other benefits of certifications as well. Firstly, certifications can set you apart from others who are competing for the same job. If you have a certification or multiple certifications, you may be chosen over someone who is equally qualified but doesn't have the certification. In these cases, the employer sees the certification as the deciding factor. That's why it's recommended for college students to pursue certifications, as it helps differentiate them from other graduates.

Accomplishment and Perseverance

Obtaining certifications also demonstrates accomplishment and perseverance. It takes hard work to earn certifications, so having them shows your commitment to your career and knowledge. Certifications are especially important when you're starting your career and have less job experience in the field. Employers not only see these certifications as evidence of your expertise, but also as a reflection of your dedication to the career.

Credibility

Certifications provide credibility. The community and employers view certifications as validation of your knowledge. Unlike simple training, a certification signifies that your expertise has been independently verified. Overall, certifications bring many benefits to your career, including better job prospects, higher salaries, differentiation from others, recognition of your commitment, and enhanced credibility.

IN-DEMAND CERTIFICATIONS
COMPTIA SECURITY+

#1
IT CERTIFICATION
in Cochise and Pima County

$74,065
Arizona median salary for jobs that ask for Security+ certification

95,000+
U.S. job openings in the last year asked for Security+

ARIZONA EMPLOYERS HIRING SECURITY+ CERTIFIED PROFESSIONALS

Raytheon
General Dynamics
Deloitte

SOS International
Northrup Grumman
Banner Health

And many more

Source: Burning Glass, last 12 months of job postings, November 2020

CERTIFICATION
ROADMAP

The somewhat complex roadmap of cybersecurity certifications is best described as a pyramid, where the basic certifications from each certification body serve as a foundation and each mastery level (intermediate, advanced, expert) adds on the body of knowledge. It is important to realize that the certifications are not only knowledge-level specific, but also category specific (i.e., communication, assets, risk management, etc.).

Explore Have your students explore the CyberSeek Interactive Tool.
https://www.cyberseek.org/certifications.html

What are the top three certifications? What are the jobs the certifications holders can aspire? What skills do students need to pass?

CERTIFICATION	JOB TITLE	TOP SKILLS

PART VI

CYBERSECURITY SCHOLARSHIP PROGRAMS

CYBERSECURITY

SCHOLARSHIP PROGRAMS

Student Cybersecurity Scholarship Programs

The cybersecurity field has several scholarship programs specifically for students pursuing a career in cybersecurity. These programs can offer scholarships that cover the cost of tuition, supplies, travel, and subsistence. Scholarships are offered based upon a wide variety of requirements. Many scholarships are designed for minority groups based on things such as race, gender, and other similar factors.

National Science Foundation CyberCorps® Scholarship Program

CyberCorps®: Scholarship for Service (SFS) is a unique program designed to recruit and train the next generation of information technology professionals, industrial control system cybersecurity professionals, and security managers to meet the needs of the cybersecurity mission for Federal, State, local, and tribal governments. The program provides scholarships through qualified institutions of higher education to students who are enrolled in cybersecurity degree programs or cybersecurity related fields. Upon graduation, scholarship recipients are required to work a period equal to the length of their scholarship in federal, state, local or tribal Government or in other approved organizations as cybersecurity professionals. Scholarships include tuition, stipend, professional allowance stipend (travel for job fair) and up to three years of support. To date, over five thousand students have received scholarships and committed to work for government organizations across the country.

CIA – Undergraduate Scholarship Program

For students interested in pursuing a government role after college, the CIA undergraduate scholarship program may be a good fit. Those attending college under the CIA's scholarship must be enrolled full time at an accredited college or university. During the summers, these students work as at the CIA. After graduation, scholarship recipients are required to work at the CIA or a period equal to 1.5 times the length of the scholarship received.

Tuition assistance up to $18,000 per calendar year for tuition, mandatory fees and books, daily allowance for meals and incidentals during summer tours, reimbursement for transportation costs between school and Washington, DC.

Stokes Educational Scholarship Program (NSA)

This is another "scholarship for service offered by NASA, meaning that the student agrees to work with the organization after graduation or else they must pay back all of the scholarship money that they have received. Recipients receive $30,000 a year for tuition. During the summers, they will intern at the NSA for 3 months.

CYBERSECURITY
SCHOLARSHIP PROGRAMS

ISC2 Scholarship – Undergraduate

The Center for Cyber Safety and Education and (ISC)2 offer both undergraduate and graduate scholarships ranging from $1,000 to $5,000 each. Anyone studying in the cybersecurity field is eligible to apply for these scholarships regardless of citizenship.

Up to 20 scholarships awarded to undergraduate applicants. If awarded the award will be sent to the school with instructions that it be applied to tuition, fees and books.

National Science Foundation CyberCorp Scholarship Program

The Snort scholarship is offered by technology giant Cisco. Those awarded the Snort scholarship receive $10,000 to be used at an accredited college, university, or institution of their choice. The only requirements for this scholarship are that the applications can obtain a high school diploma by the year the scholarship would take effect or can provide reasonable evidence that they are seeking a degree in an applicable field. The scholarship typically runs between the months of April and May. - $10,000 awarded.

American Security Professional Fellowships

Heinz College awards a minimum scholarship of $10,000 per semester up to a full tuition scholarship to eligible students. If you are interested in an American Security Professional Fellowship, you must be a U.S. citizen who plans to enroll on a full-time basis and exemplifies a strong commitment to the field of IT management.

PART VII

ESTABLISHING A CYBERSECURITY CAREER PATHWAY

WHAT ARE
CAREER PATHWAYS

Career Pathways System is about the coordination of people and resources to provide a more consistent system of education, training, and learning opportunities.

Ultimately, career pathways can be defined as a sequence of career focused classes, extra-curricular experiences, industry credentials, and workforce readiness experiences like apprenticeships or internet ships that prepare students for future careers. In a career pathway, different programs and services are combined to help students develop important skills in areas like academics, technical knowledge, and employability in the cybersecurity field.

A career pathways initiative involves partnerships between universities, four-year colleges, community colleges, primary and secondary schools, government agencies, employers, labor groups, and social service providers. These partnerships work together to coordinate training options, academic credentials, industry certifications and job placement. Well-designed career pathways try to eliminate replication of courses and subject content, lower education, and tuition cost, and give students an earlier start to reaching career goals.
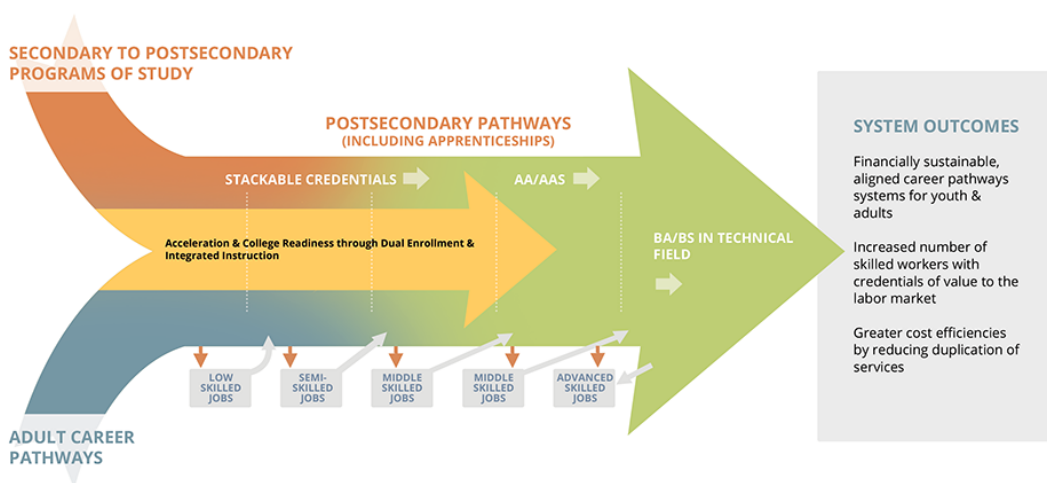
Career pathways models are used at the federal, state, and local levels. States often use different sources of funding to support the various parts of career pathways models. The Integrated Career Pathways Model below shows how a comprehensive Career Pathways System can serve both high school age youth, as well as adults, and promote collaboration, alignment, and cross-system development of structured pathways into and through postsecondary credential programs.

" **Empowering Futures: Uniting Education and Industry in Cybersecurity Career Pathways"**

WHAT ARE
CAREER PATHWAYS

Academic Articulated Credit

One of the main goals of career pathways is to allow students to earn college credits while still in high school, or while attending community college before transferring to a four-year institution. Essentially, articulation refers to the college credits that a student earns as part of an agreement between two or more educational institutions, such as high schools, community colleges, technical colleges, or universities, and their academic programs. These agreements are sometimes referred to as transfer agreements, transfer guides, or transfer pathways.

It's essential to understand that articulation agreements are seen differently by students, the institution providing the initial credits (the sender college), and the institution accepting the transfer credits (the receiving institution).

Improve Transfer Between Lower and Upper Division Academic Institutions

Articulation agreements aim to simplify the transition to college with the expectation of further enrollment in a four-year institution's program. The sender college can promote the value of their programs and courses, leveraging the reputation of the four-year institution. Meanwhile, the four-year institution can reduce recruitment costs and fill vacancies with college-ready students. The students, in turn, benefit by following specific course plans, avoiding repeating courses, and steering clear of non-applicable courses.

Colleges and universities create these articulation agreements after assessing the curriculum, program learning outcomes and instruction level. They agree on how courses completed at a community college, for example, will satisfy course requirements at a four-year institution. This process involves academic departments working together over a few months to draft and publish these guidelines.

Streamlining Course Options

Transfer agreements typically streamline course options by offering a checklist or sequence of necessary courses for degree requirements at a community college or online school. They essentially serve as roadmaps for students, removing the uncertainty about which courses to take and their transferability. Adherence to these agreements can save students both time and money, a significant advantage given the rising costs of higher education.

Transfer Articulation Agreements are usually designed for specialized professional or technical programs offered at colleges, such as Associate of Science (AS), Associate of Fine Arts (AFA), Associate of Applied Science (AAS), diplomas, and certificates. These can be applied to a specific four-year program or major at the receiving university.

WHAT ARE
CAREER PATHWAYS

High School to College Articulation Options

There are several options that allow high school students to earn college credits even before graduation. This can be incredibly advantageous, giving you a head-start on your higher education journey, especially in fast-paced fields like cybersecurity. The options include dual credit programs, dual enrollment programs, early college programs, TechPrep programs, and Advanced Placement (AP) programs.

Dual Credit Programs

Dual Credit Programs provide an opportunity for high school students to earn both high school and college credit simultaneously. This means that the coursework completed in high school counts for both your high school diploma and your future college degree.

For example, a high school might offer a dual credit program in cybersecurity where you learn about cybersecurity fundamentals including data encryption, network security access control and all other topics that align to the college class. Completing this course could count towards both your high school diploma and a future degree in cybersecurity.

Dual Enrollment Programs - Like dual credit programs, dual enrollment programs allow students to take college-level courses while still in high school. The difference is that dual enrollment credits may not always count towards high school graduation requirements. The student may also be required to take the classes at a local community college while they are still attending high school.

For instance, you could enroll in a college-level computer programming course offered by a local community college, earning college credits even before you graduate high school. There may be some restriction including application requirements, tuition requirements and age of the high school student.

Early College Programs

Early college programs, like P-TECH (Pathways in Technology Early College High School), are partnerships between high schools and colleges. These programs enable students to earn college credits alongside their high school diploma, typically starting in their junior year. Over two years, students take a mix of high school and college courses, graduating with enough credits for an associate degree. These programs are designed for students committed to an early start in a specific career area and can be hosted at the high school or a partnering community college. P-TECH, for example, allows students to graduate with a high school diploma and a no-cost associate degree in a STEM field, such as cybersecurity.

WHAT ARE
CAREER PATHWAYS

Advanced Placement (AP) Programs

Advanced Placement, or AP, is a program run by the College Board that offers college-level curricula and examinations to high school students. Colleges and universities often grant course credit to students who obtain high scores on the examinations. For example, taking AP Computer Science Principles could help you delve deeper into key principles that form the basis of cybersecurity.

In summary, high school students have several options to gain college credits while still in high school. Whether you choose dual credit, dual enrollment, early college, or AP programs, you're setting a strong foundation for your future in cybersecurity or other fields. Exploring these programs not only accelerates your education but also introduces you to potential career paths, offering a glimpse into what your future in cybersecurity might look like.

Program	Description	HS Credit	College Credit	Real-world Experience
Dual Credit	Simultaneously earn high school and college credit by taking certain courses.	Yes	Yes	Depends on the course
Dual Enrollment	Enroll in college-level courses while in high school. These credits might not count toward high school requirements.	Depends on the course	Yes	Depends on the course
Early College	Partnerships between high schools and colleges that enable students to earn substantial college credits alongside their high school diploma.	Yes	Yes, often enough for an associate degree	Depends on the program
Advanced Placement (AP)	College Board program offering college-level curricula and examinations to high school students. High examination scores can lead to college credit.	Yes, from the course	Yes, from the examination	No, typically classroom-based

Selecting The Right College Program

One of the most important decisions in build an effective career pathway is selecting a good college to earn your academic credentials. There is an abundance of college that offer degrees in and certificates in cybersecurity. How can you determine which one's have the best programs.

CENTERS OF
ACADEMIC EXCELLENCE

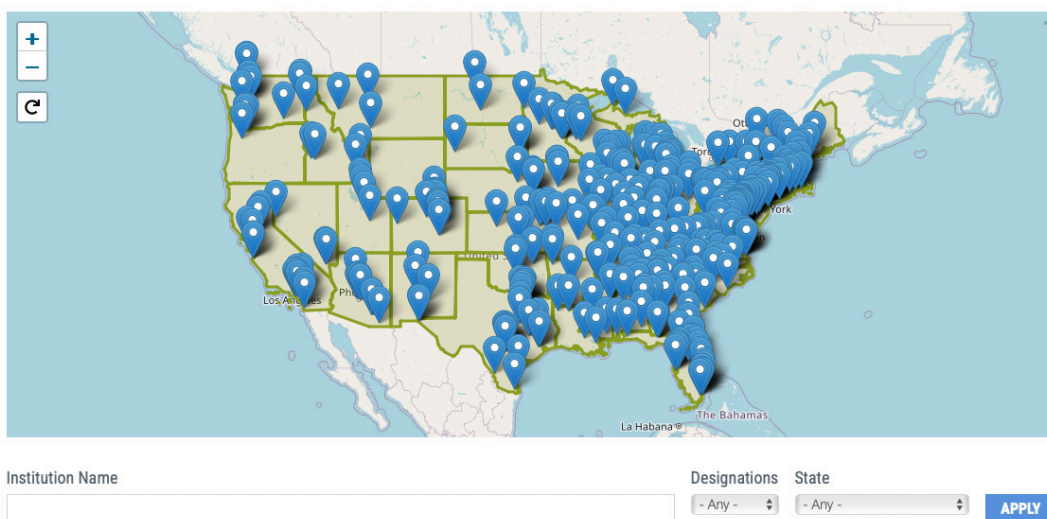## Centers of Academic Excellence in Cyber Defense

The National Security Agency's (NSA) Centers of Academic Excellence in Cyber Defense (CAE-CD) program provides an important option when selecting a college to student for a cybersecurity career. The CAE-CD program aims to produce a competent workforce to reduce vulnerabilities in our national information infrastructure. Its goal is to help train professionals who can defend against cyber threats, a pressing concern in today's data driven economy. The program encourages universities and colleges across the country to develop robust cybersecurity programs that meet high national academic standards.

CAE Program Requirements

To receive the CAE-CD designation, institutions must meet specific criteria. They must offer a cybersecurity-related degree (or similar program), have a curriculum that aligns with contribute to the advancement of the cybersecurity field. They also are required to document the success of their graduates.

Types of CAE Programs

Three different designations fall under the CAE-CD program: CAE-C, CAE-R, and CAE-O. The National CAE maintain an interactive map of all the current CAE designated institutions. The institutions are evaluated by their programs of study (POS) in cybersecurity.

WHAT ARE
PROGRAMS OF STUDY

A program of study consists of courses required to complete a specific degree, inclusive of required coursework within the major, concentration, minor and catalog.

1. **CAE-C (Center of Academic Excellence in Cyber Defense):** Institutions with this designation offer degree programs or a recognized cybersecurity focus. An example is the University of Maryland, known for its robust cybersecurity curriculum.

2. **CAE-R (Center of Academic Excellence in Cyber Defense Research):** These institutions focus on research in cybersecurity. For example, the Massachusetts Institute of Technology (MIT) is designated a CAE-R due to its extensive research in the field.

3. **CAE-O (Center of Academic Excellence in Cyber Operations):** These institutions offer an advanced, deeply technical, interdisciplinary curriculum in cyber operations. The United States Air Force Academy, which focuses on operational aspects of cybersecurity, is an example.

National Community of CAE Institutions

The community of CAE institutions across the U.S. is a strong network of education and research hubs. They collaborate on initiatives, share best practices, and contribute to enhancing cybersecurity education nationwide. This network is an important part of the national strategy to protect our digital infrastructure.

Importance of the CAE Designation for Students

Considering the CAE designation when selecting a college is crucial for aspiring cybersecurity professionals. It assures that the institution has a high-quality cybersecurity program that meets national standards. Graduating from a CAE-designated institution can make you more competitive in the job market and provide you with a solid foundation for a successful career in cybersecurity.

In conclusion, the NSA's CAE-CD program plays a vital role in producing cybersecurity professionals who are ready to protect our nation's information systems. By choosing a CAE-designated institution, you're stepping onto a path that has been carefully designed to provide the best possible education in cybersecurity.

Creating Your Unique

CAREER PATHWAYS

Are you ready to forge your unique path towards a rewarding career in cybersecurity? Let's explore the importance and the steps involved in creating a personal career pathway plan, a professional blueprint that aligns with your personal goals and aspirations.

Why is a Career Pathway Plan Important?

A career pathway plan can act as your roadmap, guiding you towards your dream job in cybersecurity. It helps you assess your strengths, work on your weaknesses, and align your interests with potential career options.

Creating Your Career Pathway Plan: A Step-by-Step Guide

1. **Self Evaluate:** Begin by assessing your strengths and weaknesses. For instance, are you good at problem-solving or coding but struggle with time management? Also, identify your interests. Do you enjoy learning about network security or are you more intrigued by ethical hacking?

2. **Explore Career Options:** Research different careers within the cybersecurity field. Look at job descriptions, requirements, and necessary skills. For instance, a cybersecurity analyst needs a strong understanding of threat identification and mitigation. They must be good problem solvers. A network security specialist design, implements and supports secure communications systems.

3. **Plan your Path:** Utilize resources available at school or online to develop your plan. This might involve meeting with teachers, career counselors or academic advisor. Ask about opportunities to earn college credit while still in high school. Take to the people that manage the college programs you are interested in pursuing. It might include visiting business that employ cybersecurity professionals or taking certain classes, participating in clubs, or seeking internships in the cybersecurity field.

4. **Engage Your Support Network:** Involve your teachers, counselors, and parents in your planning process. They can provide valuable advice and feedback on your career pathway plan. Share your plan and seek out assistance in selecting classes, preparing for industry certifications or college applications. Look for student organizations, conferences, job fairs or internship or apprentice programs.

5. **Set Personal Goals:** Define specific, measurable, achievable, relevant, and time-bound (SMART) goals. For example, you might set a goal to complete a cybersecurity certification by the end of your junior year or attend a student cybersecurity club event.

6. **Monitor Your Progress:** Regularly revisit your plan and track your progress towards your goals. Adjust your plan as needed based on your accomplishments, industry and technology trends and evolving interests.

Creating Your Unique

CAREER PATHWAYS

Further Tips for Your Career Pathway Journey

- **Stay Current with Trends:** Keep abreast of the latest developments in the cybersecurity field. This knowledge can inform your plan and help you make strategic decisions about your career pathway plan.

- **Embrace Technology:** The cybersecurity sector is intertwined with technological advancements. Stay updated on technologies like secure communications, Artificial Intelligence (AI), virtualization, smart devices, and cloud computing.

- **Fuel Your Passion:** Embrace the opportunities that a cybersecurity career pathway can offer, from competitions and internships to exchange programs. Your enthusiasm can inspire others to support your plan.

- **Network:** Building relationships your teachers, advisors, fellow students, and with professionals in the field who can offer valuable insights and potential job opportunities. Remember, networking is a two-way street; strive to assist others in their professional journeys too.

Remember, creating a personalized career pathway plan is your first step towards a fulfilling career in cybersecurity. Use this guide as a starting point and shape your unique path to success.

PART VIII

EXTRA–CURRICULAR ACTVITIES

EXTRA-CURRICULAR
ACTIVITIES

Extracurricular activities provide a channel for reinforcing the lessons learned in the classroom, offering students the opportunity to apply academic skills in a real-world context, and are thus considered part of a well-rounded education.

This is particularly important for cybersecurity students. It enables them to build skills in critical thinking, problem solving and learn to work in teams.

The Cyber Security Club is a student-run club with the goal of providing outside-of-class activities relevant to the cybersecurity industry. Student participants will leave with valuable experience proven to be useful during interviews and jobs.

Student cybersecurity competitions provide a fun and interesting way to exercise technical skills, identify and recognize cybersecurity talent, and engage students and professionals in the field. It also lets them experience how an organization must deal with the constant threat of cyber-attacks.

Popular Student Cybersecurity Competitions

1. **CyberPatriot** is a program established for the K-12 education of students in cybersecurity by the Air Force Association. There are three branches of the program, including the National Youth Cyber Defense Competition, AFA CyberCamps, and Elementary School Cyber Education Initiative. The Cyber Defense Competition starts at the state and then regional level. Top competitors are then given an all-expense paid trip to the national finals. At nationals, participants compete for national recognition and scholarship money. https://www.uscyberpatriot.org

    NICE Alignment: Operate and Maintain & Protect and Defend
    NICE Skills Alignment: System and network administration

2. **CSAW Capture the Flag (CTF)** is the most comprehensive student-run cyber security event in the world, featuring 9 hacking competitions, workshops, and industry events. Final events are hosted by 6 global academic centers. https://www.csaw.io

    NICE Alignment: Operate and Maintain & Protect and Defend
    NICE Skills Alignment: Skills vary by individual challenge.

EXTRA-CURRICULAR
ACTIVITIES

Popular Student Cybersecurity Competitions (cont.)

3. **The National Cyber League (NCL)**, powered by Cyber Skyline, enables students to prepare and test themselves against practical cybersecurity challenges that they will likely face in the workforce, such as identifying hackers from forensic data, pentesting and audit vulnerable websites, recovering from ransomware attacks, and much more! Open to U.S. high school and college students, the NCL is a community and virtual training ground that allow students to develop and demonstrate their technical cybersecurity skills, helping students bridge the gap from curriculum to career! https://nationalcyberleague.org

   NICE Alignment: Operate and Maintain & Protect and Defend
   NICE Skills Alignment: System and Network Administration

4. **MITRE Cyber Academy** presents an annual STEM Capture the Flag challenge that is open to both current students and professionals. While current professionals may compete in the competition for education and training purposes, only eligible high school and college teams are able to obtain winning prizes, scholarships, and internships. https://mitrecyberacademy.org

   NICE Alignment: Analyze and Protect and Defend
   NICE Skills Alignment: Steganography, Software Exploitation, Computer Forensics, Cryptography, Networking

5. **The NSA Codebreaker Challenge** provides students with a hands-on opportunity to develop their reverse-engineering / low-level code analysis skills while working on a realistic problem set centered around the NSA's mission. https://codebreaker.ltsnet.net/challenge

   NICE Alignment: Securely Provision & Investigate
   NICE Skills Alignment: Encryption Algorithms and Stenography, Digital Forensics, Cryptography, Networking

6. **The PicoCTF** is a free computer security game targeted at middle and high school students, created by security experts at Carnegie Mellon University. The game consists of a series of challenges centered around a unique storyline where participants must reverse engineer, break, hack, decrypt, or do whatever it takes to solve the challenge. https://picoctf.com

   NICE Alignment: Operate and Maintain & Protect and Defend
   NICE Skills Alignment: System and Network Administration