Cybersecurity Career Seekers’ Exploration Guide

When exploring cybersecurity as a career option, these questions arise:

- How much money can I make?
- What is the pathway from entry level to advanced roles?
- What skills are needed?
- What educational program should I pursue?
- By the time I graduate, what are the job prospects predicted to be?

The online tools discussed in this article are designed to explore those questions using real-time, current, job market data.

This article teaches how to map your own cybersecurity career journey using the tools at:

- Cyber.org,
- CyberSeek.org,
- The Cyber Career Pathways Tool at NICCS.

Anyone considering a cybersecurity career can benefit from this career guidance, including those who’ve already been working in IT, those with no technical background, and anyone developing a cybersecurity college plan.

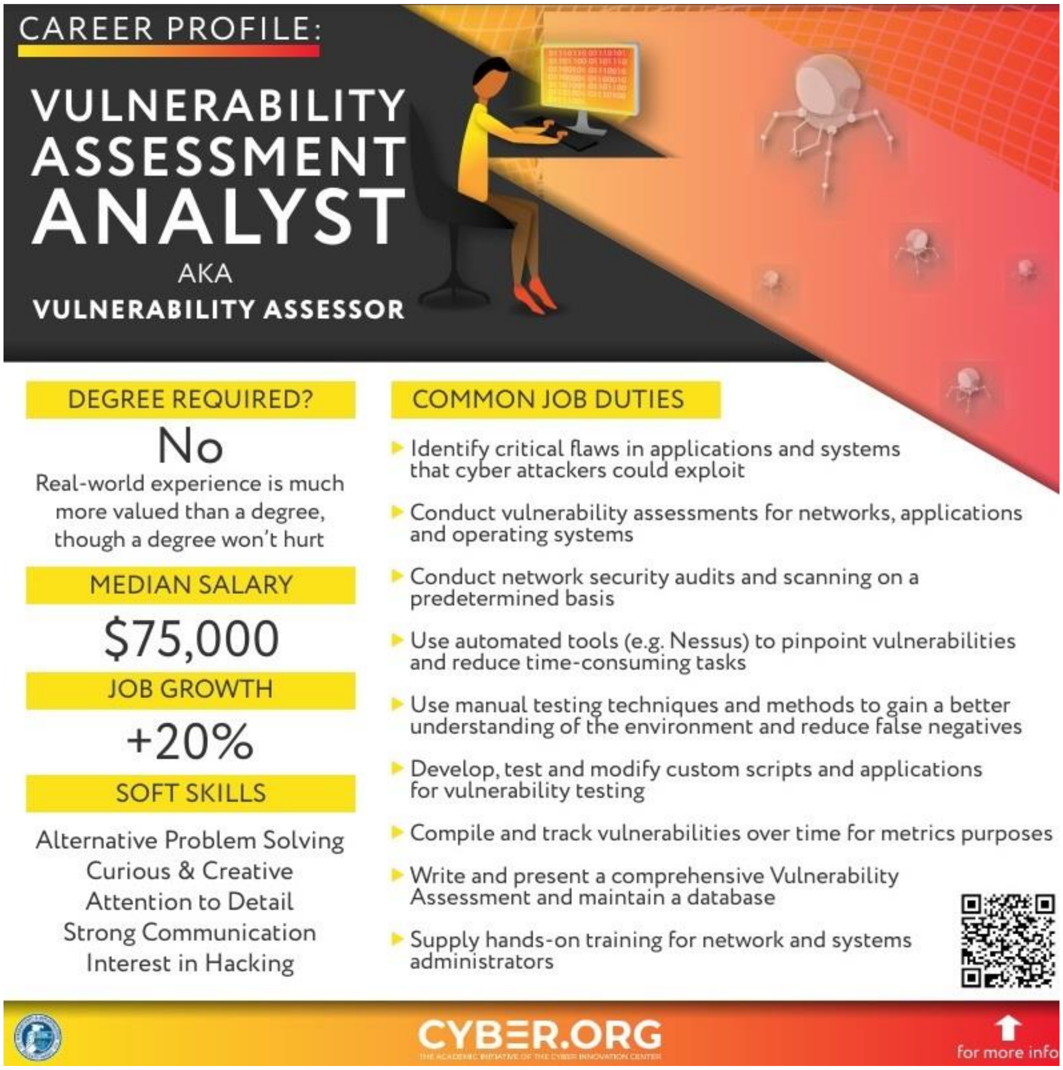
Career Pathways at Cyber.org

Cyber.org has listed 24 job roles related to cybersecurity. Each is presented like a baseball card with a colorful graphic and a high-level overview. Highlights include the **average salary, job duties, skills, educational requirements and job growth outlook**. To find them, go to **Career Exploration** and **Click on Cyber Career Profiles**.

The educational filter offers checkboxes to narrow your search based on degree requirements. For example, click on *Associate’s Degree Required*. The job titles Software Developer and Cybersecurity Engineer are displayed. Now, remove that checkmark and click *Degree Not Required*. Nine job roles are listed. Note that this is not a complete view of the industry, rather, it’s a good place to start.

To dig a little deeper, let's examine one role together: Vulnerability Assessment Analyst.

In the category of *Degree Not Required*, we find **Vulnerability Assessment Analyst**. The job's average salary is $75,000, job growth is over 20%, and its skills and duties are briefly described. You could be hired for this role without a degree if you possess the skills and have experience. Later, we'll talk about how to develop those skills.



CAREER PROFILE:

VULNERABILITY ASSESSMENT ANALYST

AKA

VULNERABILITY ASSESSOR

DEGREE REQUIRED?

No

Real-world experience is much more valued than a degree, though a degree won't hurt

MEDIAN SALARY

$75,000

JOB GROWTH

+20%

SOFT SKILLS

Alternative Problem Solving
Curious & Creative
Attention to Detail
Strong Communication
Interest in Hacking

COMMON JOB DUTIES

- Identify critical flaws in applications and systems that cyber attackers could exploit
- Conduct vulnerability assessments for networks, applications and operating systems
- Conduct network security audits and scanning on a predetermined basis
- Use automated tools (e.g. Nessus) to pinpoint vulnerabilities and reduce time-consuming tasks
- Use manual testing techniques and methods to gain a better understanding of the environment and reduce false negatives
- Develop, test and modify custom scripts and applications for vulnerability testing
- Compile and track vulnerabilities over time for metrics purposes
- Write and present a comprehensive Vulnerability Assessment and maintain a database
- Supply hands-on training for network and systems administrators

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

for more info

According to CISA (Cybersecurity & Infrastructure Security Agency), a Vulnerability Assessment Analyst performs assessments of systems and networks to identify where they deviate from acceptable configurations and\or policy. This role also measures the effectiveness of defense-in-depth architecture against known vulnerabilities. See the CISA website to read more, including the *many* different job titles applied to this role, as well as its core duties and competencies. You will do well in this role if you have an eye for detail, you are a good sleuth and have a knack for evaluating according to policies.

Community and Technical colleges can teach the core skills needed for this role. Over 30 institutions in Washington state offer cybersecurity programs. Two-year degrees as well as certificates can prepare you for an entry level cybersecurity job like this one. Salaries quickly rise as your skills increase and you advance into higher positions.

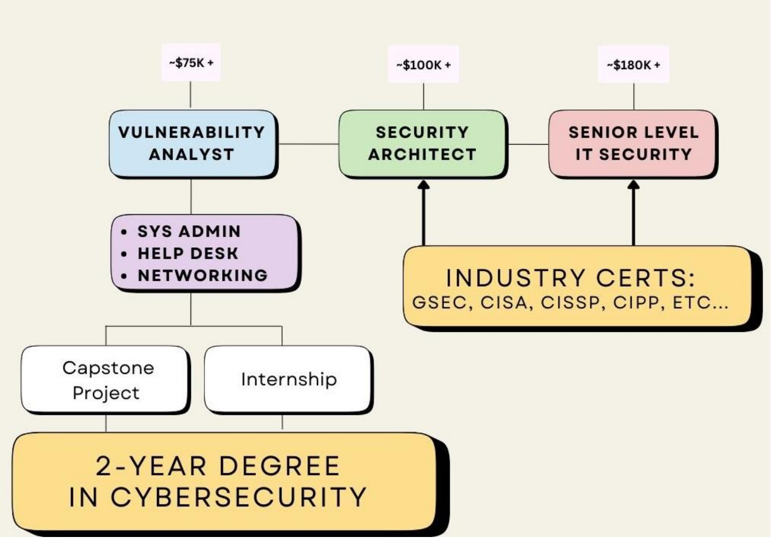
But what if a fresh graduate struggles to get hired without experience? Try something related to cybersecurity with easier entry points for people straight out of school. For example, start with a role like:

- System Administration
- Network Administration
- Quality Assurance
- Technical Support
- Software Development

The cybersecurity programs offered in Washington colleges include curriculum to teach the skills needed in these foundational roles. Any one of these jobs will sharpen your troubleshooting skills and train you to think with a security-by-design mindset, preparing you to quickly climb into a cybersecurity role.

Furthermore, in these roles, you'll gain an in-depth understanding of the company's products and infrastructure. This first-hand knowledge of how everything works is indispensable when you later become an analyst responsible for securing and protecting these assets.

After working for a while in cybersecurity, you'll be armed with the experience needed to study for and earn industry certifications. Advancement into higher roles usually requires such certificates. Look for employers that provide stipends for training and exam vouchers.



For more details about the duties and skills of a Vulnerability Analyst, read this article on CompTIA's website.

Career Pathways at CyberSeek.org

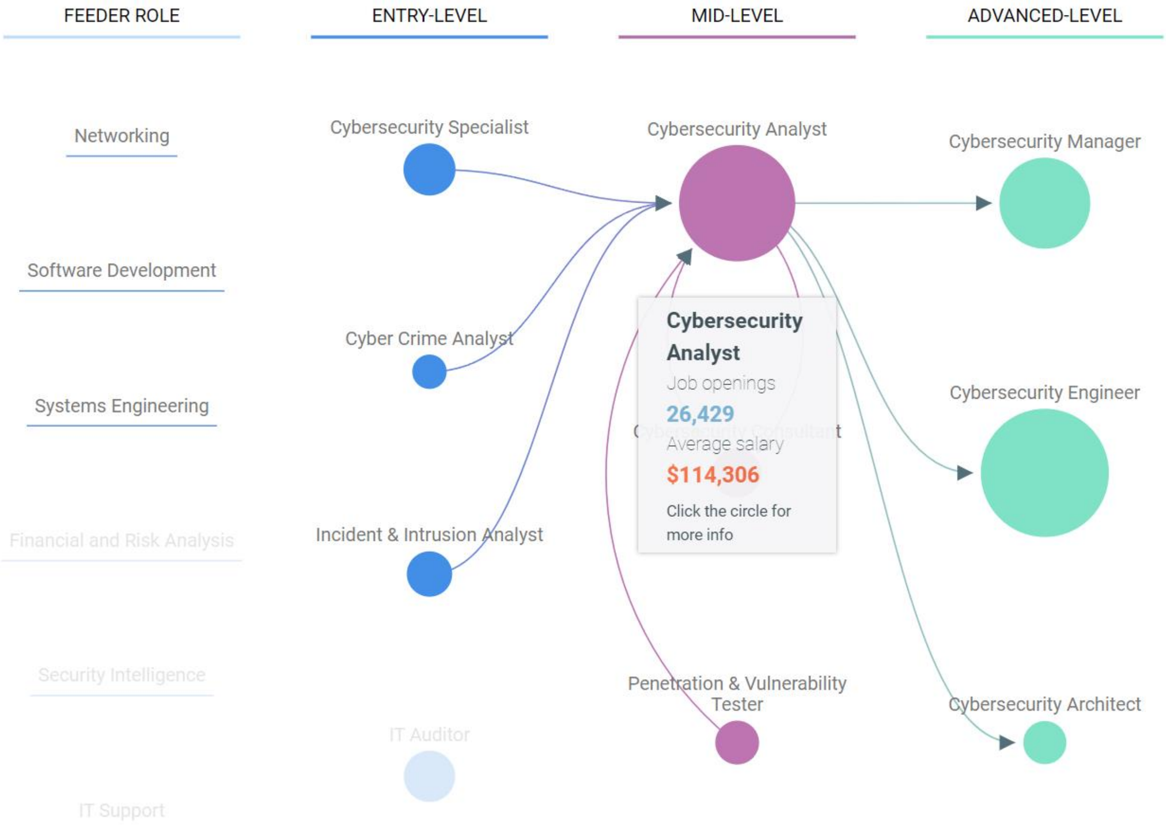
After examining the career journey of a vulnerability analyst, you understand the various stages of education and how they relate to career advancement. Now, using a similar construction path, look at the more specialized job roles at CyberSeek.org.

The mission of CyberSeek.org is to: 'provide detailed, actionable data about **supply and demand** in the cybersecurity job market.' This helps you estimate the likelihood of finding a job after investing in college and helps you develop an educational plan based on the skills you need.

The data is continually refreshed, so the following will probably change by the time you visit the website. Today it states: **"From May 2023 to April 2024, there were only 85 cybersecurity workers available for every 100 cybersecurity jobs demanded by employers."**

Click on CyberSeek's Career Pathway tool. In the Roles tab, the interactive tool helps you visualize the pathway from a "Feeder Role" up to "Advanced-Level" roles. Click any role to see information like average salary, top skills requested, total job openings over the past 12-month period, and top certifications requested.

Take special note of the "Top Future Skills Requested" section. As you shop for a college, examine the curriculum to see if these skills are covered.



Cybersecurity Analyst

Job openings

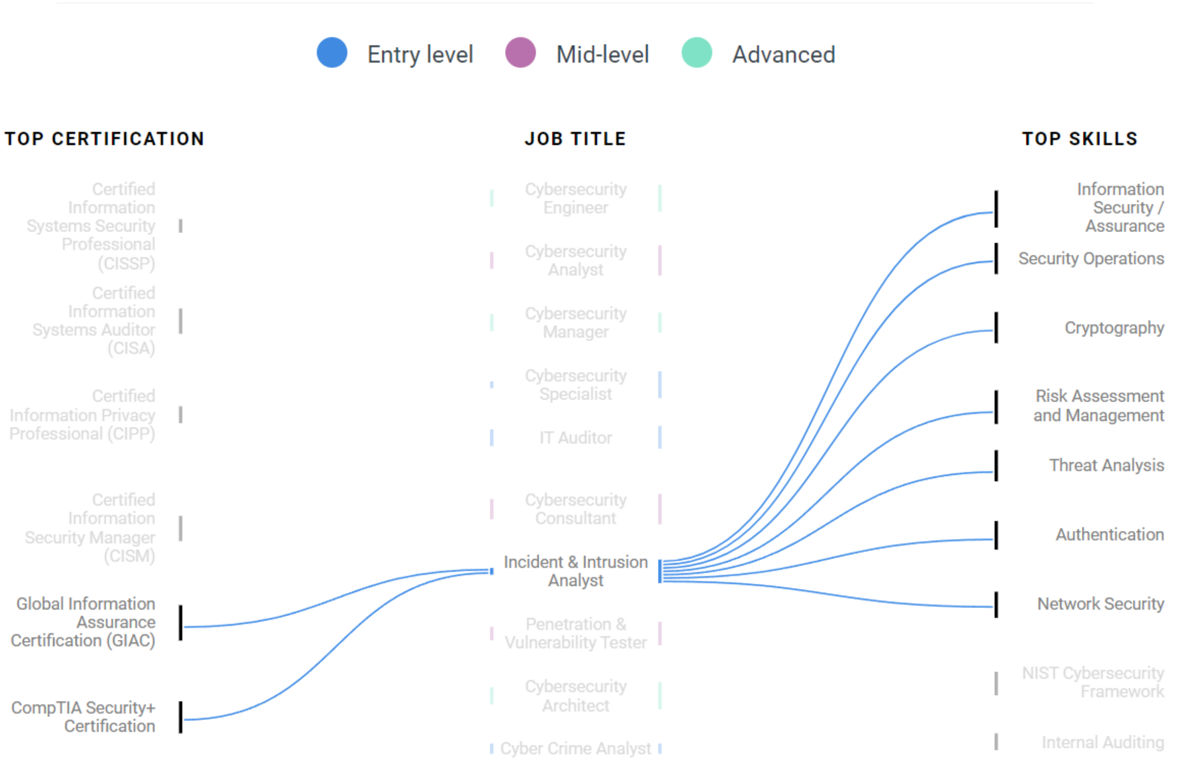
26,429

Average salary

$114,306

Click the circle for more info

The Skills and Certifications tab allows you to see dynamic connections between certifications, job titles, and skills.


● Entry level
● Mid-level
● Advanced
TOP CERTIFICATION
JOB TITLE
TOP SKILLS
Certified Information Systems Security Professional (CISSP)
Certified Information Systems Auditor (CISA)
Certified Information Privacy Professional (CIPP)
Certified Information Security Manager (CISM)
Global Information Assurance Certification (GIAC)
CompTIA Security+ Certification
Cybersecurity Engineer
Cybersecurity Analyst
Cybersecurity Manager
Cybersecurity Specialist
IT Auditor
Cybersecurity Consultant
Incident & Intrusion Analyst
Penetration & Vulnerability Tester
Cybersecurity Architect
Cyber Crime Analyst
Information Security / Assurance
Security Operations
Cryptography
Risk Assessment and Management
Threat Analysis
Authentication
Network Security
NIST Cybersecurity Framework
Internal Auditing

NICCS Framework Cyber Career Pathways Tool

The National Initiative for Cybersecurity Careers and Studies (NICCS) presents an even more comprehensive career pathways tool. Fifty-two work roles related to cybersecurity are clearly defined and organized into seven categories. This lexicon is called the NICE Framework.

Work roles are categorized by the nature of the duties performed in that role. For example, there is the “Design and Development” category which lists eight work roles. The “Protection and Defense” category has seven. The “Investigation” category lists two roles.

The NICE Framework clearly states that work roles are not synonymous with job titles. Job titles vary from place to place. Someone with one job title may perform the work of many different “roles” defined in the NICE Framework.

For example, several “roles” from the NICE Framework are needed to describe the daily job tasks performed by a **DevSecOps Solutions Architect** (which is a job title.) The “roles” performed in this highly paid job can probably be found in all seven categories of the NICE Framework.

Now that we understand more clearly what a “role” is, let’s continue our examination of the Vulnerability Analyst role. Click on Vulnerability Analysis in the green section. Browse among the tabs for more details, for example, Tasks, Knowledge and Skills. It also shows a constellation of related roles that link to Vulnerability Analysis. A single job **title** for Vulnerability Analyst on ZipRecruiter or Indeed might encompass many of these job **roles**.

The Details tab provides a link to usajobs.gov where you can search for current federal job listings related to the Vulnerability Analyst role. Here is where the differences between “role” and “job title” get fuzzy. If nothing results from searching **Vulnerability Analyst**, try some of the other "Related Functional Titles” back in the Details tab at niccs.cisa.gov, like **Cybersecurity Threat Analyst**.

In the Micro-Challenge tab, check out the hands-on activity, “Attempt Vulnerability Analysis Micro-Challenge,” where you perform a simulated security audit.

You will certainly enjoy examining other cybersecurity roles using this dynamic tool.

Selecting a Washington College

Selecting a college is probably your next step in this journey. As you shop, keep in mind that each cybersecurity degree will have its own specialty focus areas. For example, some degree programs train heavily for software development and network security, while others focus more on cloud, or industrial control systems, or mobile technology. Colleges regularly survey employers in their regions to discover the requested skill sets and develop curriculum accordingly.

You can also survey the job market in your area. Sign up with Indeed or ZipRecruiter and scan the job market for cyber-related jobs in your region. Examine the skill sets that employers seek. Also look at how many employers require a 4-year degree. Then, ask about these skills and requirements when talking to college advisors.

To make your college shopping experience easy, the Cybersecurity Center of Excellence of Washington has created a comprehensive list of Washington colleges offering cybersecurity (and related) programs. See that list at: https://coecyber.io/students. Included are certificates, two-year degrees, technical programs, and 4-year degrees. A link to each college’s website is included where you may read more and find contact information for college advisors.

We congratulate your choice to begin an exciting and well-paid career!