

BEYOND THE HACKER STEREOTYPE

**Exploring Cybersecurity Careers
You Didn't Know Existed**

BRIAN MYERS PHD, CISSP, CCSK



Experience

- 20 years in software development
- 9 years in information security

Past Positions

- InfoSec Director, WebMD Health Services
- Senior AppSec Architect, WorkBoard
- Senior Risk Advisor, Leviathan Security

Current Work

- Independent Information Security Consultant
- Co-organizer, OWASP AppSec Days PNW



English Major

English PhD



Technical Writer

Program Manager

Software Developer

Software Architect

Program Manager

Product Manager

VP of Product Dev

Manager, Software Dev

Director, Software Dev

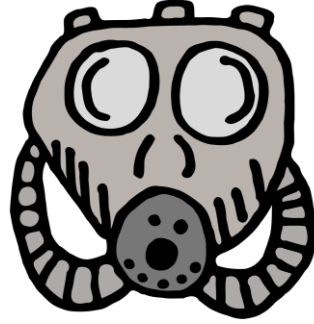


Security Architect

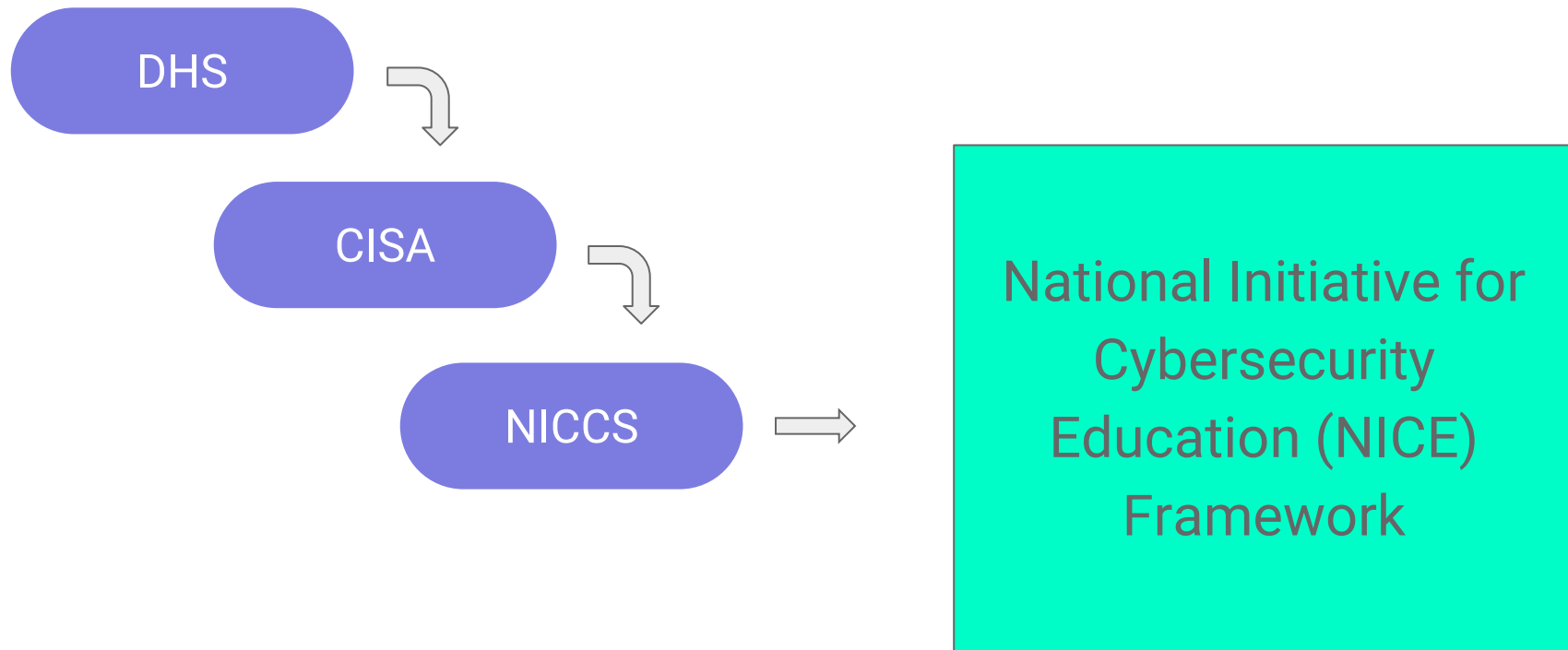
Director, Information Security

Application Security Architect

Security Consultant



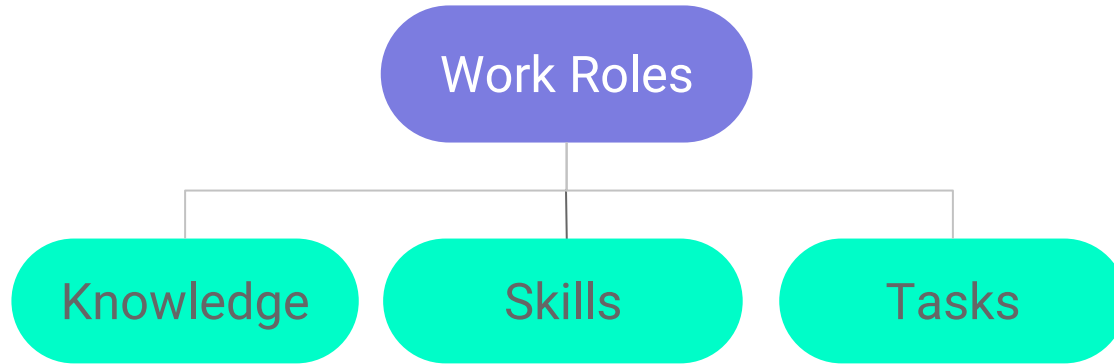
INTRODUCING THE NICE FRAMEWORK



WORK ROLE CATEGORIES

Oversight and Governance	Leadership, management, advocacy
Design and Development	Research, design, develop, test
Implementation and Operation	Configure, operate, maintain
Protection and Defense	Identify, analyze, and mitigate risks
Investigation	Investigate attacks and crimes
Cyberspace Intelligence	Collect, analyze, disseminate threat info
Cyberspace Effects	Plan and execute cyber operations

NICE FRAMEWORK



SKILLS: COMMUNICATING

Skill ID	Skill Name
S0077	Skill in securing network communications
S0182	Skill in analyzing target communications internals and externals collected from wireless LANs
S0252	Skill in processing collected data for follow-on analysis
S0283	Skill in transcribing target language communications
S0385	Skill in communicating complex concepts
S0386	Skill in communicating verbally
S0387	Skill in communicating in writing
S0483	Skill in identifying software communications vulnerabilities
S0533	Skill in developing target communication profiles
S0537	Skill in designing wireless communications systems
S0596	Skill in encrypting network communications
S0610	Skill in communicating effectively
S0716	Skill in identifying target communications networks
S0824	Skill in communicating with customers
S0825	Skill in communicating with engineering staff
S0826	Skill in communicating with external organizations
S0827	Skill in communicating with internal and external stakeholders
S0888	Skill in performing target communications analysis

ROLES WITH S0385 AND S0387

Work Role	Skill
Cybersecurity Instruction (OG-WRL-005): Responsible for developing and conducting cybersecurity awareness, training, or education.	S0097, S0156, S0379, S0380, S0381, S0385, S0386, S0387, S0388, S0389, S0390, S0391, S0392, S0393, S0394, S0395, S0424, S0430, S0431, S0467, S0468, S0472, S0473, S0483, S0530, S0543, S0544, S0572, S0591, S0592, S0597, S0600, S0601, S0602, S0610, S0612, S0613, S0618, S0628, S0629,
Security Control Assessment (OG-WRL-012): Responsible for conducting independent comprehensive assessments of management, operational, and technical security controls and control enhancements employed within or inherited by a system to determine their overall effectiveness.	S0015, S0097, S0111, S0136, S0141, S0172, S0175, S0177, S0248, S0252, S0385, S0386, S0387, S0388, S0389, S0391, S0393, S0394, S0401, S0402, S0403, S0409, S0414, S0415, S0416, S0423, S0430, S0431, S0435, S0436, S0437, S0438, S0439, S0440, S0441, S0443, S0447, S0462, S0463, S0465, S0466, S0472, S0473, S0483, S0503, S0504, S0506, S0511, S0515, S0532, S0543, S0544, S0558, S0559, S0574, S0578,
Cybersecurity Architecture (DD-WRL-001): Responsible for ensuring that security requirements are adequately addressed in all aspects of enterprise architecture, including reference models, segment and solution architectures, and the resulting systems that protect and support organizational mission and business processes.	S0141, S0172, S0383, S0385, S0386, S0387, S0418, S0419, S0428, S0429, S0430, S0458, S0465, S0466, S0543, S0544, S0551, S0569, S0570, S0571, S0574, S0578, S0590, S0596, S0598, S0613, S0632, S0637, S0638, S0655, S0657, S0658, S0659, S0673, S0674, S0675, S0683, S0685, S0686, S0728, S0762, S0791, S0813, S0814, S0822, S0853, S0880, S0893

CAREER PATHWAYS TOOL

Cybersecurity Instruction

Compare against another Work Role

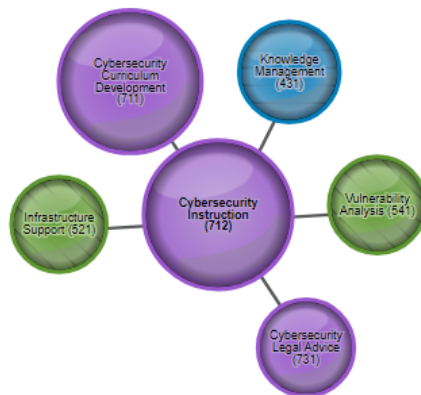
Hide Diagram



Clear selection

Begin typing to search work role names. Or [search job titles](#).

[Search job titles](#).



Details

Spotlight Videos

Task statements

Knowledge and Skill statements

Capability Indicators

Common Relationships

Federal Data

Cybersecurity Instruction

Responsible for developing and conducting cybersecurity awareness, training, or education.

Community: Cross Functional

Category: Oversight and Governance

OPM ID: 712

[See USAJOBS listings coded for Cybersecurity Instruction](#)

Related Functional Titles

The following job titles have been identified by subject matter experts as either alternative titles for this work role or including the functions of this work role as part of their job duties.

- Cyber Field Instructor (CFI)
- Cyber Professor
- Cyber Trainer
- Cyber Training Specialist
- Cyber Workforce Developer
- Information Security Trainer
- Learning Officer
- Security Training Coordinator

Related NICCS Education & Training Catalog Courses

- [New Horizons ISO/IEC 27001 Foundation](#)
- [New Horizons ISO 22301 Foundation](#)

Details

Spotlight Videos

Task statements

Knowledge and
Skill statements

Capability
Indicators

Common
Relationships

Federal Data

Cybersecurity Instruction

Related Functional Titles

The following job titles have been identified by subject matter experts as either alternative titles for this work role or including the functions of this work role as part of their job duties.

- Cyber Field Instructor (CFI)
- Cyber Professor
- Cyber Trainer
- Cyber Training Specialist
- Cyber Workforce Developer
- Information Security Trainer
- Learning Officer
- Security Training Coordinator

Details

Spotlight Videos

Task statements

Knowledge and
Skill statements

Capability
Indicators

Common
Relationships

Federal Data

Legend

C - Core Task

A - Additional Task

A* - Not included in the initial analysis to determine whether it is Core or Additional to the work role.

C	T0101	Evaluate the effectiveness and comprehensiveness of existing training programs
A	T1008	Prepare and deliver education and awareness briefings
A	T1009	Create a cybersecurity awareness program
C	T1020	Determine the operational and safety impacts of cybersecurity lanes

Details

Spotlight Videos

Task statements

Knowledge and
Skill statements

Capability
Indicators

**Common
Relationships**

Federal Data



Related Roles by TKS

On Ramps

Off Ramps

The following work roles are related by their shared task, knowledge, and skill statements.

711-Cybersecurity Curriculum Development

87.38%

431-Knowledge Management

40.98%

541-Vulnerability Analysis

36.73%

731-Cybersecurity Legal Advice

36.07%

CAPABILITY INDICATORS

	Entry	Intermediate	Advanced
Education	Associate's, Bachelor's	Bachelor's	Bachelor's, Master's, Ph.D.
Training	Talent Development, Human Resources, Technical	IT, Cyber, Instructional Design, Vendor, LMS	Instructional Design, Learning Styles, IT
Credentials / Certifications	Not recommended	Beneficial, not essential	Recommended

ROLE: CYBERSECURITY INSTRUCTION



Jamal Mercer (He/Him) · 3rd

Engagement Coordinator and Speaker at
Microsoft's Cybercrime Center

ROLE: CYBERSECURITY LEGAL ADVICE

TASKS

Evaluate regulatory compliance

Align policies with regulatory requirements

Determine the impact of security lapses

Evaluate regulatory changes

SKILLS

Evaluate laws

Evaluate policies

Assess risks

Communicate well

KNOWLEDGE

Security and privacy laws

Risk management process

Supply chain risks

Federal agency roles

Cyber principles and practices

ROLE: CYBERSECURITY LEGAL ADVICE

- Attorney-Adviser
 - Contract Attorney
 - Foreign Law Specialist
 - General Attorney
- Attorney-Adviser
 - Contract Attorney
 - Foreign Law Specialist
 - General Attorney



Molly Buckley

LEGAL FELLOW

Molly Buckley is a Legal Fellow on EFF's civil liberties team, where she works on free speech, privacy, censorship, and surveillance issues.

ROLE: CYBERSECURITY LEGAL ADVICE

DEGREE REQUIRED?

Yes

Juris Doctorate Degree
is required

MEDIAN SALARY

\$92,000

JOB GROWTH

28%

SOFT SKILLS

Good communicator

Good listener

Approachable

Interpersonal skills

COMMON JOB DUTIES

- ▶ Advocate for an organization in legal and legislative proceedings
- ▶ Evaluate contracts
- ▶ Evaluate regulations, policies and procedures
- ▶ Interpret and apply laws
- ▶ Resolve conflicts in policies and procedures
- ▶ Maintain a working knowledge of relevant constitutional issues
- ▶ Evaluate the impact of changes to laws and regulations
- ▶ Help implement changes to laws
- ▶ Provide legal guidance to management, personnel, or clients

ROLE: KNOWLEDGE MANAGEMENT

TASKS

Manage knowledge repositories

Create knowledge assets

Make knowledge access paths

Protect access to assets

Monitor usage of assets

SKILLS

Conduct searches

Conduct research

Administer databases

Perform technical writing

KNOWLEDGE

Knowledge management tools

Collaboration tools

Taxonomy of models and frameworks

Security principles and practices

IR principles and practices

ROLE: KNOWLEDGE MANAGEMENT

- Business Analyst
- Business Intelligence Analyst/Manager
- Business and Requirements Analyst
- Content Manager
- Data Custodian
- Data Storage Specialist
- Information Manager
- Information Owner/Steward
- Records and Information Management Specialist



megan barker ✓ · 2nd

Senior Security Specialist, Documentation at 1Password

ROLE: KNOWLEDGE MANAGEMENT

DEGREE REQUIRED?

No

But Bachelor's Degree
is recommended
Certifications encouraged

MEDIAN SALARY

\$75,000

JOB GROWTH

11%

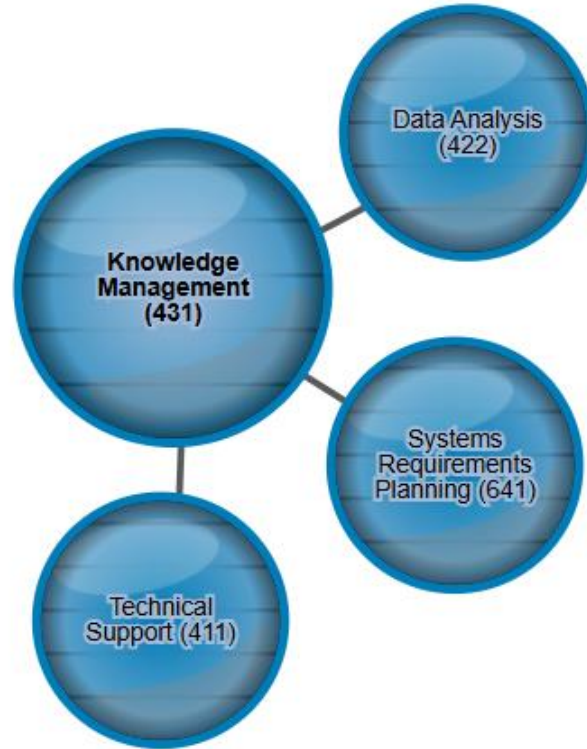
SOFT SKILLS

Multitasking
Leadership
Big-picture vision
Responsible

COMMON JOB DUTIES

- ▶ Help organizations to identify, document, and access intellectual assets like employee expertise, best practices, and organizational knowledge
- ▶ Perform information searches, knowledge mapping, and knowledge management
- ▶ Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy
- ▶ Ensuring compliance with Payment Card Industry and Personal Health Information data security standards
- ▶ Design, build, implement, and maintain a knowledge management framework that provides end-users access to the organization's intellectual capital
- ▶ Promote knowledge sharing between information owners/users through an organization's operational processes and systems
- ▶ Lead efforts to promote the organization's use of knowledge management and information sharing

★ BONUS FEATURE: ON RAMPS ★



ROLE: THREAT ANALYSIS

TASKS

Monitor websites for hostile content

Identify threat tactics

Coordinate collection activities

Prepare threat briefings

Assess effectiveness of intelligence

SKILLS

Conducting deep web research

Collaborating with others

Analyzing large data sets

Mimicking threat actors

Establishing priorities

KNOWLEDGE

Cognitive biases

Security threats

Network principles

Web security principles

Intelligence fusion

ROLE: THREAT ANALYSIS

- Threat Analyst
- Cyber Intelligence Analyst
- Security Analyst
- Incident Response Analyst



Daria-Romana P.  · 2nd
Threat Intelligence Analyst @ Microsoft

ROLE: THREAT ANALYSIS

DEGREE REQUIRED?

Yes

Bachelor's in Cybersecurity
IT, or Computer Science

Certifications Encouraged

MEDIAN SALARY

\$119,000

JOB GROWTH

30%

SOFT SKILLS

Collaborative
Ability to Work Well
Under Pressure
Analytical

COMMON JOB DUTIES

- ▶ Provide subject matter expertise to the development of cyber operations-specific indicators
- ▶ Monitor open source websites for hostile content directed towards organizational or partner interests
- ▶ Collaborate with intelligence analysts and targeting organizations involved in related areas
- ▶ Conduct in-depth research and analysis
- ▶ Use gathered intelligence to counter incoming threats and prevent potential threats
- ▶ Provide current intelligence support to critical internal/external stakeholders as appropriate
- ▶ Identify threat tactics and methodologies
- ▶ Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations

ROLE: CYBERCRIME INVESTIGATION

TASKS

Process crime scenes

Interview witnesses

Analyze network attacks

Process digital evidence

Assess behavior of suspects during investigations

Prepare reports

SKILLS

Navigate the dark web

Examine digital media

Collect digital evidence

Assess supply chain risk

Solve problems

Analyze behavior

Analyze threats

KNOWLEDGE

Cyber laws and regulations

Security principles and practices

Authentication techniques

Intrusion detection tools

Adversarial techniques

Abnormal behavior

ROLE: CYBERCRIME INVESTIGATION

- Computer Crime Investigator
- Cyber Incident Handler / Responder
- Special Agent



Marqwuese Bayne · 3rd

Sr. U.S. Probation Officer at U.S. Probation
Office: Cybercrime Specialist

ROLE: CYBERCRIME INVESTIGATION

DEGREE REQUIRED?

NO

Certification(s) encouraged
but not essential
Experience can supplement

MEDIAN SALARY

+\$67,000

JOB GROWTH

10%

SOFT SKILLS

Curiosity & Persistence
Strong Communication
Information Use
Critical Thinking

COMMON JOB DUTIES

- ▶ Find and navigate the dark web
- ▶ Process crime scenes
- ▶ Conduct interviews of victims, witnesses, and/or suspects
- ▶ Examine recovered data for information
- ▶ Fuse computer network attack analyses with criminal and counterintelligence investigations and operations
- ▶ Determine whether a security incident is indicative of a violation of law that requires specific legal action
- ▶ Identify elements of proof of the crime
- ▶ Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents, investigations, and operations
- ▶ Provide criminal investigative support to trial counsel during the judicial process
- ▶ Prepare reports to document the investigation

★ BONUS FEATURE: JOB LISTINGS ★

[See USAJOBS listings coded for Cybercrime Investigation](#) 

USAJOBS

Criminal Investigator

Office of Inspector General

Department of Education

Multiple Locations

Starting at \$105,029 Per Year (GS
13)

Permanent • Full-time



 Open 10/21/2024 to 11/04/2024

ROLE: MULTI-DISCIPLINED LANGUAGE ANALYSIS

TASKS

Transcribe language materials

Advise on cultural issues

Develop intel collection strategies

Identify technologies used by target

Identify foreign language terms in software code

SKILLS

Transcribe communications

Identify customer needs

Assess threat actors

Perform OSINT research

Analyze social networks

Interpret traceroute results

KNOWLEDGE

Languages & dialects

Linguistic analysis

Analytical tools and techniques

Network communications principles

Laws and regulations

Digital communications systems

ROLE: MULTI-DISCIPLINED LANGUAGE ANALYSIS

- Language Intelligence Analyst
- Foreign Language Analyst
- Linguistic Analyst
- Content Analyst



Ernest Song · 3rd

Cyber Threat Intelligence Analyst / Linguist

ROLE: MULTI-DISCIPLINED LANGUAGE ANALYSIS

DEGREE REQUIRED?

Yes

Bachelor's Degree
in target language is encouraged
if applicant is not a native speaker

MEDIAN SALARY

\$55,000

JOB GROWTH

42%

SOFT SKILLS

Good Communicator

Detail-oriented

Analytical

Identify contexts & subtleties
in written & verbal communications

COMMON JOB DUTIES

- ▶ Analyze and process information using language and cultural expertise
- ▶ Compile and interpret data for intelligence
- ▶ Assess a target's motivation and frame of reference for intelligence context
- ▶ Analyze metadata to look for patterns, anomalies, or events
- ▶ Identify cyber threat tactics
- ▶ Identify foreign languages and dialects in initial source data
- ▶ Help optimize the development of language processing tools
- ▶ Analyze social network activities
- ▶ Translate voice and graphic data
- ▶ Identify cyber or technology-related terminology used in target languages

ROLE: EXPLOITATION ANALYSIS

- Vulnerability Analyst
- Penetration Tester
- Security Researcher
- Security Engineer
- Offensive Security Engineer
- Red Team Operator
- **Vigilante Hacker by Night**



Elliot Alderson

Cyber Security Engineer at AllSafe

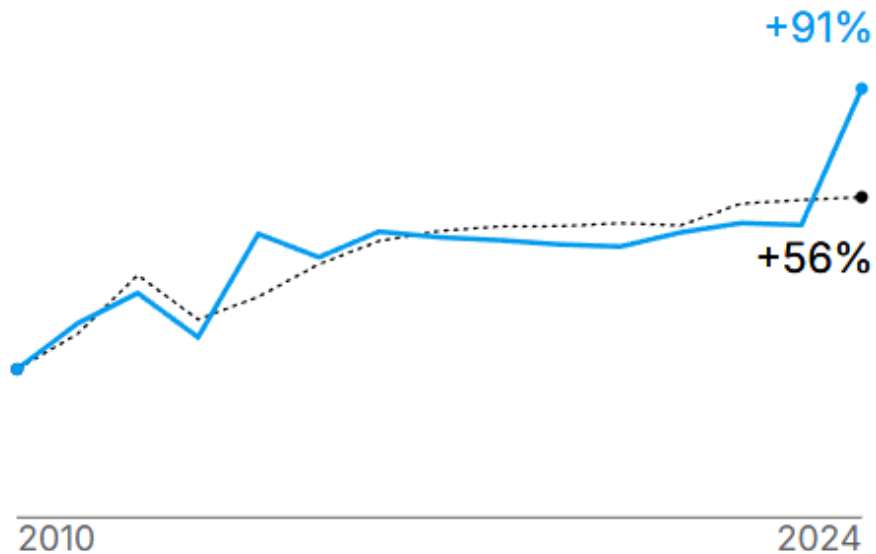
REVIEW

- NICE Framework (from NICCS)
- Cybersecurity Instruction
- Cybersecurity Legal Advice
- Knowledge Management
- Threat Analysis
- Cybercrime Investigation
- Multi-disciplined Language Analysis

HISTORICAL EMPLOYED CYBERSECURITY WORKFORCE ⓘ

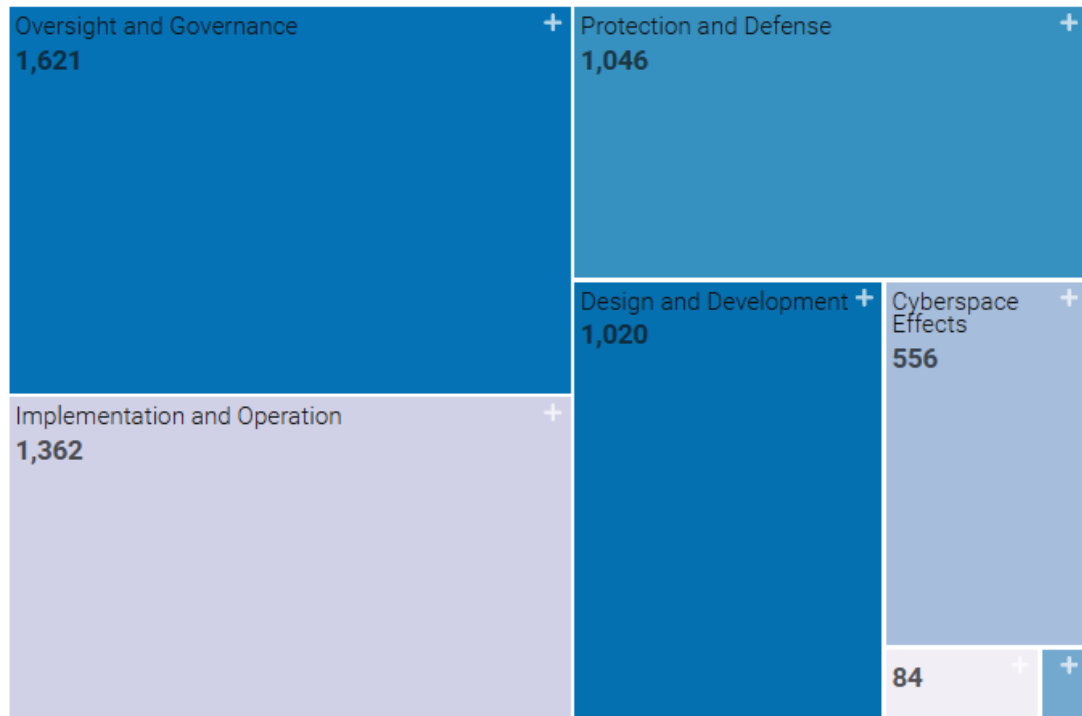
NATIONAL AVG

PORTLAND-VANCOUVER-HILLSBORO, OR-WA

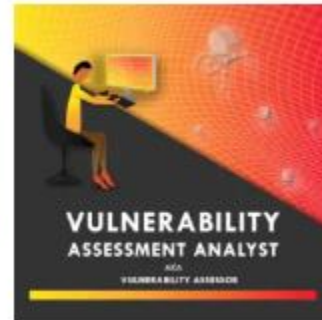


CYBERSEEK.ORG

NICE



Our country needs individuals with cybersecurity skills at all levels of every organization, in all industries, from finance and healthcare to entertainment.



RESOURCES

The logo for the National Initiative for Cybersecurity Careers and Studies (NICCS). It features the word "NICCS" in a large, bold, serif font, with a registered trademark symbol (®) to its upper right.

NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

niccs.cisa.gov

Info on security careers,
education, and training

The logo for Cyber Seek. It features a white circular icon with a stylized 'C' and a location pin symbol, followed by the words "Cyber Seek" in a bold, sans-serif font.

cyberseek.org

Detailed data about security job
market supply and demand



NWCYBER

PAVING THE WAY TO CAREERS IN CYBERSECURITY

nwcyber.org (*coming soon*)

We inform, connect, and guide
people to opportunities

QUESTIONS?

LICENSE AND ATTRIBUTION

This material is licensed under the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Attribution: Please credit Brian Myers.

NonCommercial Use Only: Internal use permitted. Commercial use prohibited.

For full license terms, visit:

<https://creativecommons.org/licenses/by-nc/4.0>