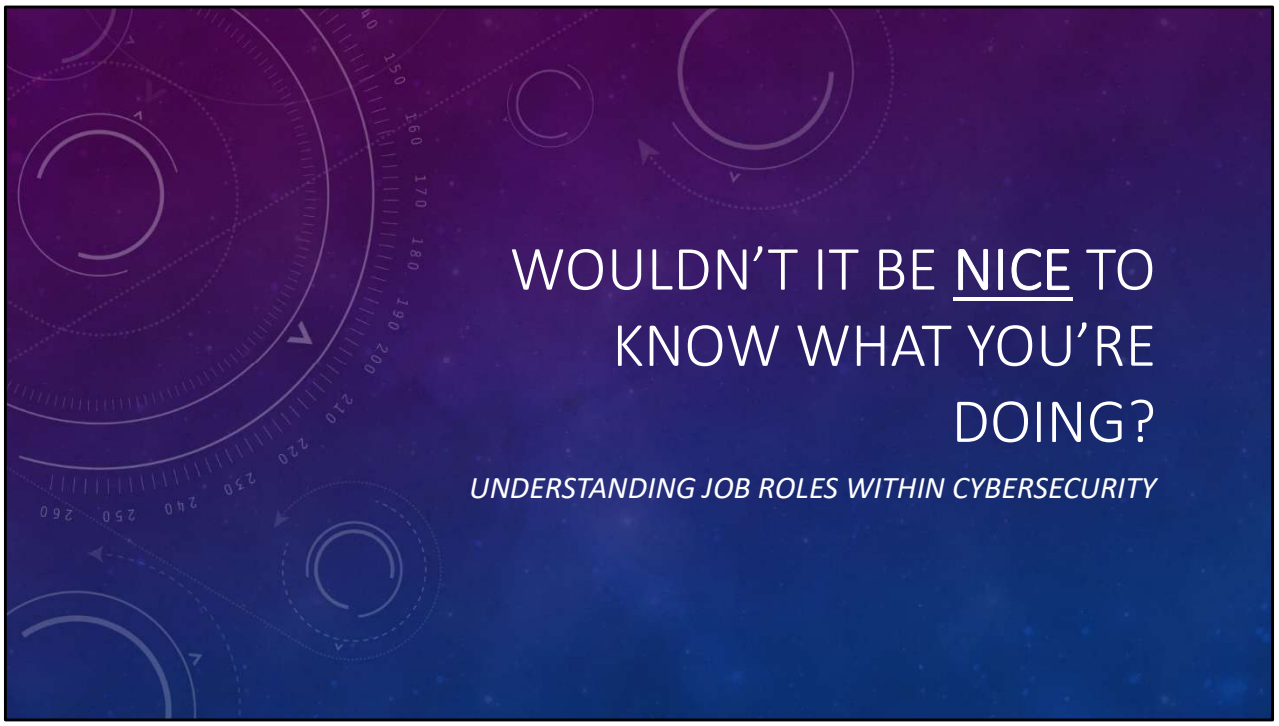

WOULDN'T IT BE NICE TO KNOW WHAT YOU'RE DOING?
UNDERSTANDING JOB ROLES WITHIN CYBERSECURITY

You think there are thousands of jobs out there? No.

How many people in your year are graduating this year?

LETS LOOK AT CYBERSECURITY

Employed: ~15200

West Australian: 6.9%

"Suitability Gap"

262112 "ICT Security Specialist"

Listed as a Shortage due to Suitability Gap

> “Shortages exist when employers are unable to fill or have considerable difficulty filling vacancies for an occupation, or ***significant specialised skill*** needs within that occupation, at current levels of remuneration and conditions of employment and in reasonably accessible locations.”
>
> - Jobs & Skills Australia
>
> https://www.jobsandskills.gov.au/data/occupation-shortages-analysis

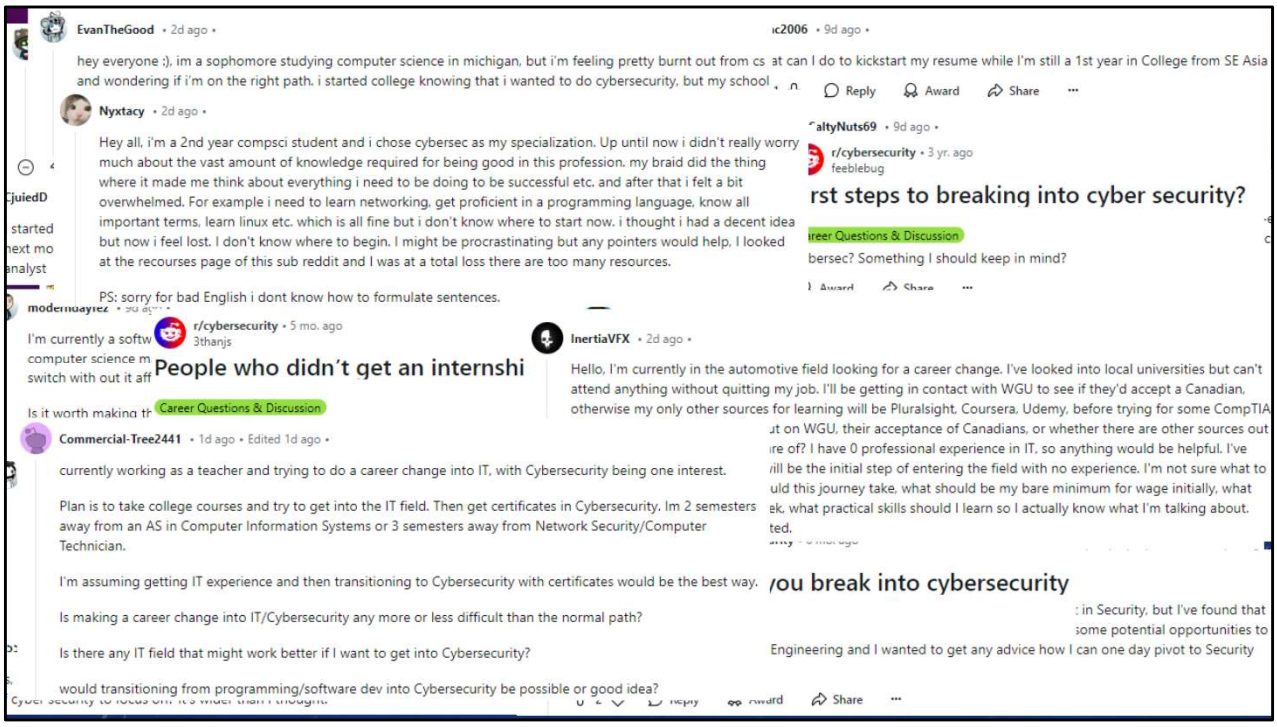
The skills that employers are looking for are not the same as

- Your Interests
- What you’re learning at Uni

“HOW DO I BREAK INTO CYBER?”

“WHAT DO I STUDY TO LEARN CYBER?”

“WHAT CERTS ARE BEST FOR AN ENTRY-LEVEL CYBER JOB?”


EvanTheGood • 2d ago •
hey everyone :), im a sophomore studying computer science in michigan, but i'm feeling pretty burnt out from cs and wondering if i'm on the right path. i started college knowing that i wanted to do cybersecurity, but my school
Nyxtacy • 2d ago •
Hey all, i'm a 2nd year compsci student and i chose cybersec as my specialization. Up until now i didn't really worry much about the vast amount of knowledge required for being good in this profession. my braid did the thing where it made me think about everything i need to be doing to be successful etc. and after that i felt a bit overwhelmed. For example i need to learn networking, get proficient in a programming language, know all important terms, learn linux etc. which is all fine but i don't know where to start now. i thought i had a decent idea but now i feel lost. I don't know where to begin. I might be procrastinating but any pointers would help. I looked at the recourses page of this sub reddit and I was at a total loss there are too many resources.
PS: sorry for bad English i dont know how to formulate sentences.
ıc2006 • 9d ago •
at can I do to kickstart my resume while I'm still a 1st year in College from SE Asia
Reply
Award
Share
altyNuts69 • 9d ago •
r/cybersecurity • 3 yr. ago
feeblebug
rst steps to breaking into cyber security?
ireer Questions & Discussion
bersec? Something I should keep in mind?
r/cybersecurity • 5 mo. ago
3thanjs
People who didn't get an internshi
Career Questions & Discussion
InertiaVFX • 2d ago •
Hello, I'm currently in the automotive field looking for a career change. I've looked into local universities but can't attend anything without quitting my job. I'll be getting in contact with WGU to see if they'd accept a Canadian, otherwise my only other sources for learning will be Pluralsight, Coursera, Udemy, before trying for some CompTIA
Commercial-Tree2441 • 1d ago • Edited 1d ago •
currently working as a teacher and trying to do a career change into IT, with Cybersecurity being one interest.
Plan is to take college courses and try to get into the IT field. Then get certificates in Cybersecurity. Im 2 semesters away from an AS in Computer Information Systems or 3 semesters away from Network Security/Computer Technician.
I'm assuming getting IT experience and then transitioning to Cybersecurity with certificates would be the best way.
Is making a career change into IT/Cybersecurity any more or less difficult than the normal path?
Is there any IT field that might work better if I want to get into Cybersecurity?
would transitioning from programming/software dev into Cybersecurity be possible or good idea?
ut on WGU, their acceptance of Canadians, or whether there are other sources out
ıre of? I have 0 professional experience in IT, so anything would be helpful. I've
ill be the initial step of entering the field with no experience. I'm not sure what to
uld this journey take, what should be my bare minimum for wage initially, what
ek, what practical skills should I learn so I actually know what I'm talking about.
ted.
ou break into cybersecurity
: in Security, but I've found that
some potential opportunities to
Engineering and I wanted to get any advice how I can one day pivot to Security
Share

“HOW DO I BREAK INTO CYBER?”

What does that even mean?

Cybersecurity isn’t just *one* role, but an ecosystem of roles. Where do you start?

Use:

- NICE Framework – NIST 800-181
- Cybersecurity Roles = Tasks (Skills + Knowledge)

We’re asking the wrong questions

National Initiative for Cybersecurity Education

WHAT IS THE NICE FRAMEWORK?

- **Clarify Career Paths**: Breaks cybersecurity into specific, actionable roles.
- **Bridge the Skills Gap**: Helps students, employees, and employers align training, hiring, and development.
- **Promote Workforce Development**: Enables individuals to identify where they fit and how to grow.

The Framework demystifies cybersecurity by:
Defining job categories and specialty areas.
Outlining the tasks you'll be expected to perform.
Helping you focus your studies and professional development.

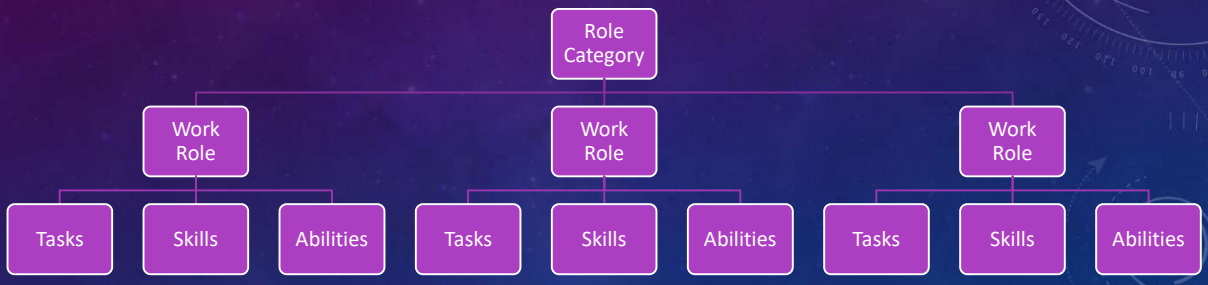
This is a framework that I've used to help build and develop teams that I've been part of

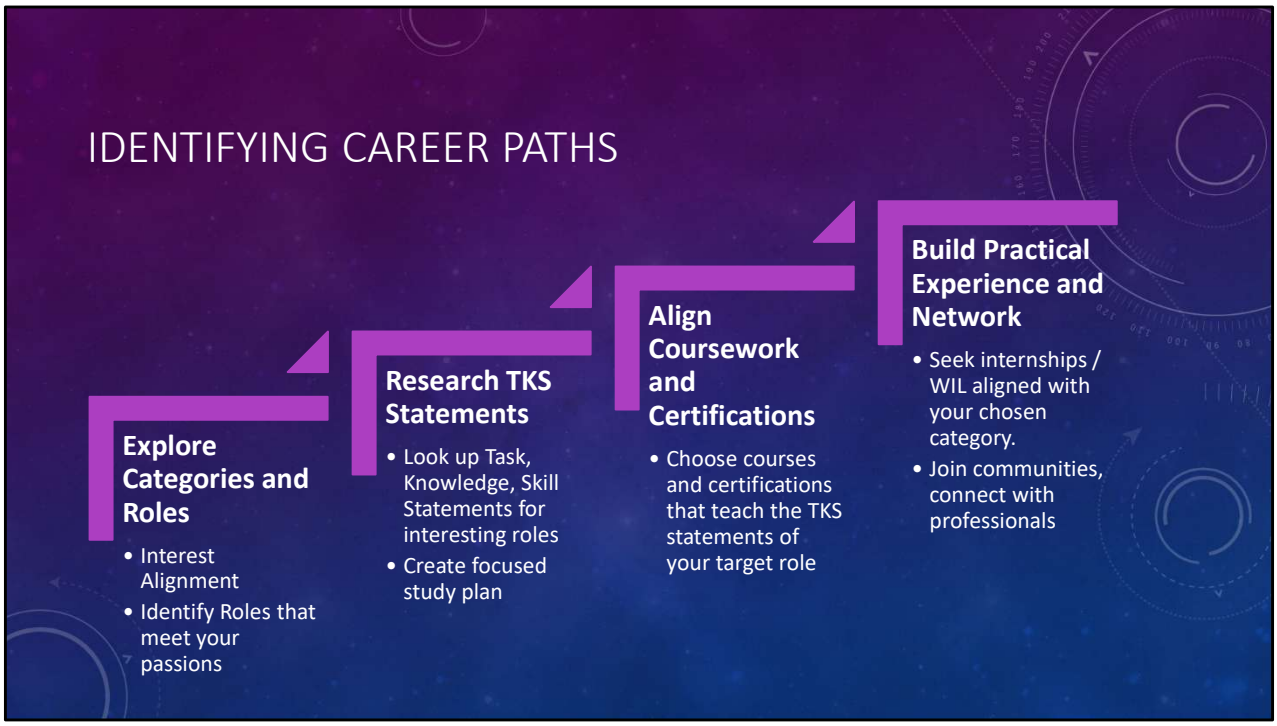
NICE HAS HELPED ME:

- Grow and develop as a professional
- Build a strong and robust team
- Get paid right

NICE FRAMEWORK

Cybersecurity Roles = Tasks (Knowledge + Skills)





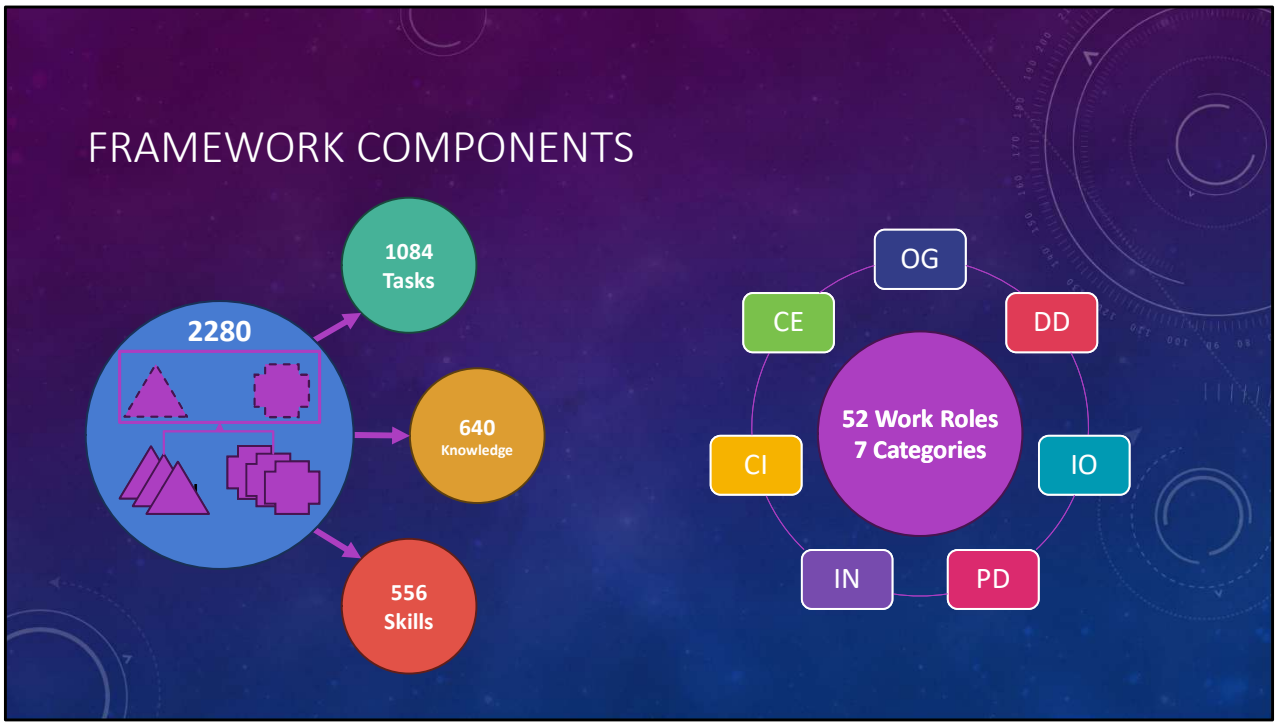
Explore Categories and Roles
Research TKS Statements – don't talk about aligning coursework
Align Coursework and Certifications

PROFESSIONALS AUSTRALIA – IT / CYBER UNION

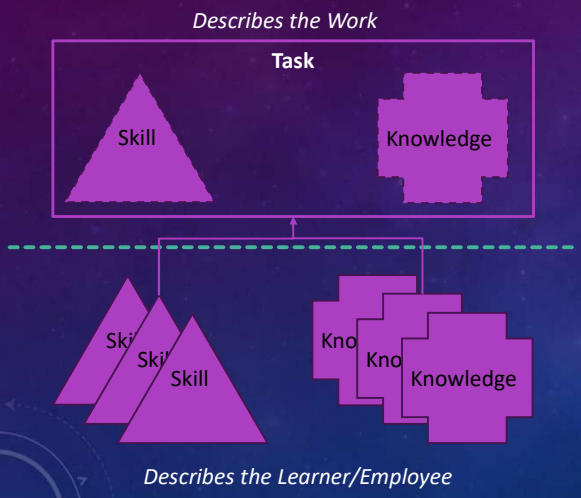
- Gain access to career support, mentorship, and professional development resources.
  - Be part of a community that advocates for fair pay, job security, and work-life balance.
  - Collective bargaining ensures your voice is heard in salary and workplace negotiations.
- **Young Professionals Australia (YPA)**
  - Designed for students and early-career professionals.
    - Connect with mentors and professionals in your field.
    - Get access to training, industry events, and career advice.
    - Support in navigating your first job, contracts, and salary negotiations.

https://www.professionalsaustralia.org.au/_YPAus

FRAMEWORK COMPONENTS



NICE COMPONENTS



Task, Knowledge, and Skill (TKS) Statements: The core building blocks of the NICE Framework.

- **Task**: An activity directed toward the achievement of organisational objectives. Task statements define the work to be done and include associated Knowledge and Skill statements that represent learners' potential to perform those Tasks.
- **Knowledge**: A retrievable set of concepts within memory. Knowledge statements define what a learner knows.
- **Skill**: The capacity to perform an observable action. Skill statements define what a learner can do.

Tasks:- Example: Monitor networks for suspicious activity.
Knowledge:- Example: Understanding attack vectors and methodologies.
Skills:- Example: Analyzing network traffic for anomalies.

TKS statements break down roles into concrete components to guide training and skill development.

NICE COMPONENTS

- **Work Role**: A grouping of work for which an individual or team is responsible or accountable. They comprise a group of Tasks that define the work to be done.
- **Work Role Categories**: High level grouping of Work Roles that fulfil a common function.

OG – Instruction, Privacy Compliance, Security Control Assessment
DD – Architecture, Software Development, R&D
IO – Data Analysis, DB Administration, Network Ops
PD – Forensics, Incident Response
IN – Cybercrime
CI – All-Source Analysis
CE – Exploitation Analysis, Cyberspace Operations

This isn't the standard – CyBOK, SFIA – but a good starting point

Section 3.3 of NIST 800-181 R1. This section is more relevant for educators.

PUTTING IT INTO PRACTICE

I want to be a SOC Analyst, what do I need to Know?

DEFENSIVE CYBERSECURITY (EXCERPT)

Responsible for analyzing data collected from various cybersecurity defense tools to mitigate risks.

Tasks	Skills	Knowledge
T0020: Develop content for cyber defence tools	**K0018**: Knowledge of encryption algorithms	**S0572:** Skill in detecting host- and network-based intrusions
T0164: Perform cyber defense trend analysis and reporting	**K0068**: Knowledge of programming language structures and logic	**S0600**: Skill in collecting relevant data from a variety of sources
T0292: Recommend computing environment vulnerability corrections	**K0692**: Knowledge of vulnerability assessment tools and techniques	**S0809**: Skill in utilising cyber defence service provider information
T0299: Identify network mapping and operating system (OS) fingerprinting activities	**K0717**: Knowledge of network access control (NAC) systems and software	**S0867**: Skill in performing malicious activity analysis
T1020: Determine the operational and safety impacts of cybersecurity lapses	**K0772**: Knowledge of systems testing and evaluation tools and techniques	**S0892**: Skill in performing trend analysis

S0572 - SKILL IN DETECTING HOST- AND NETWORK-BASED INTRUSIONS

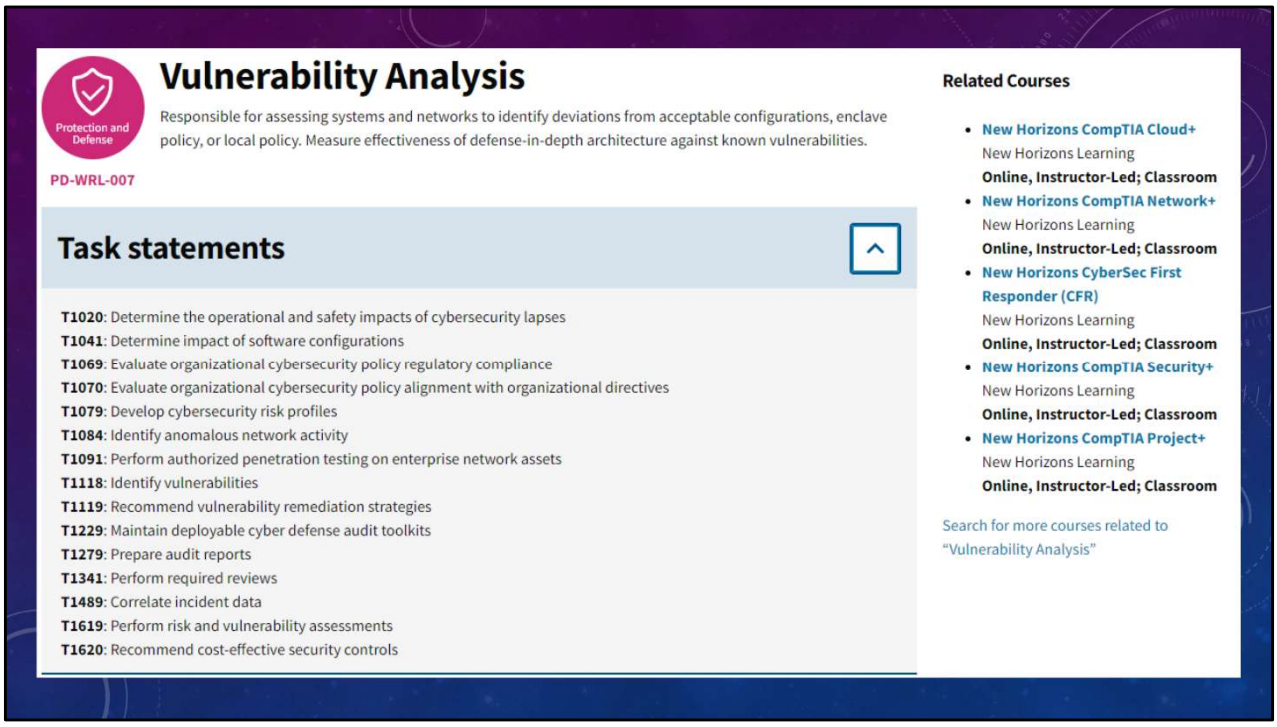
Cybersecurity Instruction:
- *Category: Oversight and Governance*
- Responsible for developing and conducting cybersecurity awareness, training, or education.

Systems Security Management
- *Category: Oversight and Governance*
- Responsible for managing the cybersecurity of a program, organization, system, or enclave.

Defensive Cybersecurity
- *Category: Protection and Defense*
- Responsible for analyzing data collected from various cybersecurity defense tools to mitigate risks.

Incident Response
- *Category: Protection and Defense*
- Responsible for investigating, analyzing, and responding to network cybersecurity incidents.

Vulnerability Analysis
- *Category: Protection and Defense*
- Responsible for assessing systems and networks to identify deviations from acceptable configurations, enclave policy, or local policy. Measure effectiveness of defense-in-depth architecture against known vulnerabilities.


Protection and Defense
Vulnerability Analysis
Responsible for assessing systems and networks to identify deviations from acceptable configurations, enclave policy, or local policy. Measure effectiveness of defense-in-depth architecture against known vulnerabilities.
PD-WRL-007
Task statements
T1020: Determine the operational and safety impacts of cybersecurity lapses
T1041: Determine impact of software configurations
T1069: Evaluate organizational cybersecurity policy regulatory compliance
T1070: Evaluate organizational cybersecurity policy alignment with organizational directives
T1079: Develop cybersecurity risk profiles
T1084: Identify anomalous network activity
T1091: Perform authorized penetration testing on enterprise network assets
T1118: Identify vulnerabilities
T1119: Recommend vulnerability remediation strategies
T1229: Maintain deployable cyber defense audit toolkits
T1279: Prepare audit reports
T1341: Perform required reviews
T1489: Correlate incident data
T1619: Perform risk and vulnerability assessments
T1620: Recommend cost-effective security controls
Related Courses
New Horizons CompTIA Cloud+
New Horizons Learning
Online, Instructor-Led; Classroom
New Horizons CompTIA Network+
New Horizons Learning
Online, Instructor-Led; Classroom
New Horizons CyberSec First Responder (CFR)
New Horizons Learning
Online, Instructor-Led; Classroom
New Horizons CompTIA Security+
New Horizons Learning
Online, Instructor-Led; Classroom
New Horizons CompTIA Project+
New Horizons Learning
Online, Instructor-Led; Classroom
Search for more courses related to "Vulnerability Analysis"

Knowledge / Skill ID	Description	Training Provider / Course	Status	Notes
S0483	Identifying software communications vulnerabilities	XYZ University - Cybersecurity Communications (Unit 101)	In Progress	Currently focusing on common vulnerabilities in APIs
S0492	Performing threat environment analysis	Threat Landscape Analysis - CyberDef Institute	Not Started	Plan to start after completing NAC fundamentals
S0532	Analyzing software configurations	Software Security Certification - SecureCode Academy	Completed	Completed via SecureCode Academy certification in 2023
K0717	Knowledge of network access control (NAC) systems and software	NAC System Fundamentals - NetworkPro Academy	In Progress	Coursework covering 50% of NAC fundamentals so far
K0728	Knowledge of Confidentiality, Integrity and Availability (CIA) principles and practices	CIA Principles & Practices - XYZ University (Unit 201)	Completed	Unit covered during previous semester
K0683	Knowledge of cybersecurity vulnerabilities	Vulnerability Assessment Workshop - SecLab	Not Started	Need to enroll in the next available workshop
K0684	Knowledge of cybersecurity threat characteristics	Cyber Threats and Indicators - Sentinel Learning	In Progress	Active participation in internal threat briefings
K1079	Knowledge of web application security risks	Web App Security Fundamentals - WebSecure Academy	Not Started	Course available next semester

Learning is just the beginning. The same framework that helps students plan their careers also supports employers in building effective teams

•As learners target roles using NICE, employers can leverage the same framework to:

- •Define roles clearly within their organisation.
- •Develop teams strategically by creating structured growth paths.

Let's take a look at how I used the NICE Framework in my own organisation to **align roles, build competencies, and foster professional growth.**

HOW WE USED NICE TO ALIGN OUR JOB ROLES

BREAKING DOWN TKS STATEMENTS

Process:

- Analyzed the **Tasks, Knowledge, and Skills (TKS) statements** for each relevant role.
- Developed **Junior and Senior assessment criteria** based on these TKS statements.

Impact:

- Created structured **criteria for promotions**.
- Allowed the team to **track growth** toward higher roles using NICE-mapped competencies.

BUILDING PROFESSIONAL DEVELOPMENT PATHWAYS

Process:

- **Mapped competencies** to Professional Development goals.
  - Example: If a role required advanced threat hunting, staff could request **relevant training** aligned to the competency.
- Ensured every team member had a **clear growth pathway** with actionable steps.

Impact:

- Team members felt more confident **asking for training** and had **better success** getting it approved.
- Created **targeted learning plans** that aligned with **career growth and role expectations**.

LEVERAGING COMPETENCIES FOR SALARY AND PROMOTION DISCUSSIONS

Process:

- Team members could **track progress** toward Senior-level criteria.
- Competencies provided a **tangible framework** for:
  - **Requesting promotions** and salary increases.
  - **Justifying salary negotiations** by showing how they met or exceeded role expectations.

Impact:

- Made salary discussions more **objective and transparent**.
- Team felt **empowered** to negotiate based on **demonstrated competencies**.

FINAL THOUGHTS

Use NICE to:

- **Clarify job roles** and align expectations.
- **Streamline professional development** pathways.
- Improve **training requests** and increase the likelihood of approval.
- Empower staff to **negotiate promotions and salaries** with confidence.

THANK YOU

https://github.com/Oscar-Geare/presentations-and-papers/tree/main/NICE%20for%20Students%20and%20Employers

https://niccs.cisa.gov/workforce-development/nice-framework