NICE Framework Application Rubric

Assessing Career Pathway Understanding and Work Role Connections

Rubric Overview

This rubric assesses students' understanding of how activity experiences connect to authentic cybersecurity careers as defined by the NICE Workforce Framework for Cybersecurity.

Use with: All three "True Teamwork" activities **Point range**: 3-12 points (3 criteria × 1-4 points each)

Assessment Criteria

Criterion 1: Work Role Recognition (1-4 points)

Score	Descriptor	Observable Behaviors
4 - Advanced	Identifies multiple relevant Work Roles and distinguishes between them	Names specific roles; explains how different roles contribute differently; recognizes role boundaries
3 - Proficient	Identifies relevant Work Roles	Can name 1-2 roles that align with activity; understands basic role functions
2 - Developing	Partial role awareness	Vague references to cybersecurity jobs; doesn't use NICE terminology
1 - Emerging	No role recognition	Cannot connect activity to career pathways

NICE Framework Work Roles addressed in these activities:

- Cyber Defense Analyst (PR-CDA-001)
- Incident Responder (PR-CIR-001)
- Vulnerability Assessment Analyst (PR-VAM-001)
- Cyber Policy and Strategy Planner (OV-SPP-002)

Criterion 2: Real-World Connection (1-4 points)

Score	Descriptor	Observable Behaviors
4 - Advanced	Makes sophisticated connections to professional practice	Explains how professionals use similar skills; identifies where human-AI collaboration appears in real work

Score	Descriptor	Observable Behaviors
3 - Proficient	Connects activity to professional work	Recognizes activity mirrors real cybersecurity tasks; can give examples
2 - Developing	General awareness	Knows activity relates to "cybersecurity jobs" but lacks specificity
1 - Emerging	No connection made	Treats activity as purely academic exercise

Criterion 3: Skill Identification (1-4 points)

Score	Descriptor	Observable Behaviors
4 - Advanced	Identifies specific skills developed and how they apply to careers	Names technical and soft skills; explains transferability; recognizes human-AI collaboration as skill
3 - Proficient	Identifies relevant skills	Can name skills practiced; understands career relevance
2 - Developing	Partial skill awareness	Identifies some skills but may miss collaboration aspects
1 - Emerging	No skill identification	Cannot articulate what was learned

Skills demonstrated across activities:

- Technical: Log analysis, incident response, policy development
- Collaboration: Human-AI partnership, team coordination
- Critical thinking: Evidence evaluation, decision-making under uncertainty
- Communication: Stakeholder communication, documentation

Scoring Guide

Total Score	Performance Level	Interpretation
10-12	Exemplary	Student demonstrates strong career awareness; consider mentorship or advanced opportunities
7-9	Proficient	Student understands career connections; encourage continued exploration
4-6	Developing	Student needs more explicit career connection instruction; provide additional resources
3	Beginning	Student has not yet connected activity to careers; revisit career framing

Activity-Specific Work Roles

Security Detective Teams

- Primary: Cyber Defense Analyst
- Secondary: Cyber Crime Investigator

AI-Assisted Incident Response

- Primary: Incident Responder
- Secondary: Cyber Defense Analyst, Security Operations Center Analyst

Ethics in Automated Security

- Primary: Cyber Policy and Strategy Planner
- Secondary: Privacy Officer, Security Governance Specialist

Instructor Notes

Integration strategies:

- Reference NICE roles explicitly during activity introduction
- Connect debrief discussions to career pathways
- Provide NICE Framework resources for interested students

Resources for students:

- NICE Framework Resource Center
- CyberSeek Career Pathways

Part of "True Teamwork: Building Human-AI Partnerships for Tomorrow's Cyber Challenges" - NICE K12 2025