Human-AI Partnership Activities for K-12 Cybersecurity Education

From the NICE K12 Cybersecurity Education Conference 2025

Three complete, classroom-ready activities, each with four grade-band versions spanning K-2 through 9-12, designed to reshape how students understand AI in cybersecurity.

The Core Idea

These activities guide students beyond viewing AI as merely a tool and toward understanding it as a **collaborative partner** in cybersecurity work.

Old Thinking	New Thinking
Humans **use** AI tools	Humans **and** AI work as teammates
AI is either adversary or tool	AI serves as a collaborative partner
Individual competency matters	Partnership capability matters

Why this matters: Contemporary cybersecurity depends on humans and AI working in concert. Students benefit from understanding what each partner contributes, as well as what neither can accomplish alone.

ℹ Learn More: The Theory Behind "AI as Partner"

This framing draws from **posthuman educational theory**, which challenges us to see technology not as something we simply *use*, but as something we *work with*. Rosi Braidotti's foundational work and Catherine Adams' practical heuristics for "interviewing digital objects" inform how these activities position AI as a collaborative teammate with distinct capabilities and limitations.
Explore the research →

The Three Activities

Activity	Focus	Grade Bands
1. Security Detective Teams	Combining AI pattern recognition with human contextual insight	K-2, 3-5, 6-8, 9-12
2. Ethics in Automated Security	Developing governance frameworks for AI security systems	K-2, 3-5, 6-8, 9-12
3. AI-Assisted Incident Response	Coordinating team roles alongside AI under time pressure	K-2, 3-5, 6-8, 9-12

Each activity comes with complete lesson plans, student materials, assessment rubrics, and strategies for classrooms with limited technology access.

Browse All Activities

Supporting Materials

Assessments

Rubrics designed around human-AI collaboration competencies, with explicit connections to the NICE Framework.

View Assessments

Implementation Guides

Practical guidance for AI platform setup alongside strategies for classrooms with limited or no AI access.

View Guides

Career Connections

One-page handouts that link each activity to authentic cybersecurity career pathways.

View Career Connections

Printables

Ready-to-print worksheets, evidence packets, and AI response cards for immediate classroom use.

View Printables

Download Everything

All materials are available as PDFs and editable DOCX files for offline use and classroom printing.

Go to Materials

Framework Alignment

Every activity connects to NICE Workforce Framework Work Roles and CYBER.org K-12 Standards. Individual activity pages provide specific alignment details.

For CTE Cybersecurity Programs

These activities align directly with Career and Technical Education pathways:

CTE Need	How These Materials Help
Industry-aligned skills	Activities mirror authentic SOC workflows and incident response procedures
NICE Framework mapping	Every activity explicitly connects to Work Roles (PR-CDA-001, PR-CIR-001, OV-SPP-002)

CTE Need	How These Materials Help
Career exploration	One-page career connection handouts link activities to real job pathways
Employer expectations	Human-AI collaboration is now standard in enterprise security operations

The 9-12 versions provide technical depth appropriate for cybersecurity pathway courses, while 6-8 versions work well for exploratory CTE programs.

For Outreach Programs

Research centers, universities, and community organizations can deploy these materials with K-12 partners:

- **Turnkey delivery** — Complete lesson plans require minimal customization
- **Scalable** — Works for single classroom visits or semester-long partnerships
- **Flexible technology requirements** — Low-resource options mean any partner school can participate
- **Assessment-ready** — Rubrics help document learning outcomes for grant reporting
- **Train-the-trainer friendly** — Materials are detailed enough for partner teachers to run independently

STEAM Integration

These activities connect naturally across disciplines:

- **Science** — Pattern recognition, hypothesis testing, evidence analysis
- **Technology** — AI systems, cybersecurity tools, network concepts
- **Engineering** — Systems thinking, incident response procedures, policy design
- **Arts** — Communication design, stakeholder messaging, ethical reasoning
- **Mathematics** — Data analysis, probability (false positives), timeline reconstruction

The investigation and policy design activities work especially well in interdisciplinary or project-based learning contexts.

Conference Session: What to Expect

ℹ Session Format (45 Minutes)

Attendees will **experience one activity as learners**, then receive access to the complete K-12 curriculum repository with dedicated implementation planning time.

Phase	Time	What Happens
Experience	20 min	Participate in one complete activity (Middle School Phishing Response Team)
Materials Tour	10 min	Overview of curriculum ecosystem and implementation guide walkthrough

Planning	10 min	Select grade-appropriate activities and begin implementation planning
Resources	5 min	Access repository, follow-up support information, Q&A

What you take home: Complete access to all 12 lesson plans, assessment rubrics, printable materials, and implementation guides—ready for immediate classroom use.

About These Materials

These resources were developed for the NICE K12 Cybersecurity Education Conference 2025 session presented by Ryan Straight, Rob Honomichl, and Paul Wagner from Cyber Operations in the College of Information Science at the University of Arizona.

Contact: ryanstraight@arizona.edu **ORCID**: 0000-0002-6251-5662

Learn More

Limited Technology Access? No Problem.

These activities function effectively at any level of AI access, including none at all. The Low-Resource Implementation Guide offers strategies that frequently produce richer learning experiences than live AI access.