Activity 1: Security Detective Teams

Building Human-AI Partnerships in Cybersecurity Investigation (Grades 6-8)

Dr. Ryan Straight

2025-12-07

Security Detective Teams

Discovering Complementary Human-AI Strengths in Cybersecurity Investigation

! Instructor Overview

This activity positions AI as a **team member** with unique capabilities and limitations, not as a tool or adversary. Students work in pairs with an AI partner to investigate security incidents, discovering how human intuition and AI pattern recognition complement each other in real-world cybersecurity scenarios.
Duration: 45-50 minutes **Grade Levels**: 6-8 (with differentiation options) **Group Size**: Pairs or small groups (3-4 students) **Technology Requirements**: At least one device per group with internet access

i Implementation Timeline

First Time Teaching This Activity: ~90 minutes prep
- Review materials & try AI prompts yourself (30 min)
- Print evidence packets & worksheets (15 min)
- Set up devices & test AI access (15 min)
- Pre-teach vocabulary: incident, pattern recognition, credential (30 min, day before)

Subsequent Uses: ~30 minutes prep
- Print materials & refresh on scenario (15 min)
- Quick device check (15 min)

Pro Tip: Print evidence packets double-sided to save paper and mimic real "case files."

Learning Objectives

Primary Objective

Students will identify and articulate the complementary strengths of human and AI team members in cybersecurity investigation tasks.

NICE Framework Alignment

- **Cyber Defense Analysis**: Analyze log data and identify patterns

- **Investigation**: Conduct systematic security investigations
- **Threat Analysis**: Evaluate potential security threats

CYBER.org Standards (Supplemental)

- **6-8.SEC.AUTH**: Authentication and access control
- **6-8.SEC.INFO**: Information security principles
- **6-8.DC.THRT**: Threat identification and analysis
- **6-8.DC.ETH**: Ethical considerations in cybersecurity

Career Pathway Connections

Students explore Work Roles: SOC Analyst, Incident Responder, Digital Forensics Analyst

Pre-Activity Setup

Classroom Preparation Checklist

- ☐ Test AI platform access (ChatGPT, Claude, or alternative)
- ☐ Print investigation packets (1 per group)
- ☐ Prepare role assignment cards
- ☐ Set up demonstration station
- ☐ Create shared documentation space (Google Docs, OneNote, etc.)
- ☐ Review AI interaction protocols with co-presenter (if applicable)

AI Platform Setup Options

High-Resource Environment

- Individual or paired student accounts for ChatGPT/Claude
- Direct student interaction with AI
- Real-time collaboration features enabled

Medium-Resource Environment

- Shared class account projected on screen
- Groups submit questions through teacher
- Rotate device access among groups

Low-Resource Environment

- Teacher demonstrates AI interactions
- Pre-generated AI responses for key questions
- Focus on analysis rather than direct interaction

The Investigation Scenario

The Case: Mysterious Account Lockouts at Cyber Academy Middle School

Background: Over the past week, several student accounts at Cyber Academy Middle School have been locked out due to failed login attempts. The IT department has gathered evidence and needs your detective team to investigate.

CC BY 4.0

Your Mission: Work with your AI partner to analyze the evidence, identify patterns, and determine if this is a security incident or a coincidence.

Evidence Available: 1. Login attempt logs showing timestamps and usernames 2. Password complexity report for affected accounts 3. Social media activity from affected students 4. Help desk tickets from the past month 5. Network activity logs from suspicious time periods

Investigation Materials

Evidence Packet Contents

Document A: Login Logs

USERNAME	DATE	TIME	ATTEMPTS	STATUS
jsmith2025	11/18/25	3:45 AM	12	LOCKED
mgarcia2025	11/18/25	3:47 AM	15	LOCKED
kchen2025	11/19/25	3:44 AM	8	LOCKED
rjones2025	11/19/25	3:46 AM	10	LOCKED
tpatel2025	11/20/25	2:15 PM	3	SUCCESS

Document B: Password Analysis

USERNAME	COMPLEXITY	LAST_CHANGED	PATTERN_DETECTED
jsmith2025	WEAK	8/15/25	Birthday-based
mgarcia2025	WEAK	8/15/25	Pet name + year
kchen2025	WEAK	8/15/25	School name + numbers
rjones2025	MEDIUM	10/01/25	Random with substitutions
tpatel2025	STRONG	11/01/25	Passphrase

Document C: Social Media Clues

Recent posts from affected students show: - Birthday celebrations with dates visible - Pet photos with names in captions - School spirit posts with mascot references - Favorite sports teams and player numbers

Document D: Network Observations

- All failed attempts originated from IP: 203.45.67.89
- Geolocation: Outside normal school district
- Time pattern: 3:44-3:47 AM (except one)
- User agent: Automated tool detected

Student Investigation Worksheet

Part 1: Human Detective Work

Before consulting your AI partner, examine the evidence and record:

1. **Initial Observations** (What patterns do you notice?)
   - Time patterns: _____
   - Account similarities: _____
   - Password patterns: _____

CC BY 4.0

2. **Human Intuition** (What feels suspicious or important?)
   - _____
   - _____
3. **Questions for AI Partner** (What would you like AI to help analyze?)
   - _____
   - _____

Part 2: AI Partnership Investigation

AI Interaction Protocol: Frame your AI as a team member, not a search engine.

⚠ What AI Can and Can't Do

AI is GOOD at (share Documents A, B, D with AI):
- Finding patterns in structured data (login timestamps, IP addresses)
- Identifying password complexity issues
- Recognizing known attack signatures

AI is NOT good at (YOU analyze Document C):
- Understanding WHY someone posted on social media
- Reading social context and intentions
- Knowing if birthday posts are innocent or oversharing

HUMANS are NOT good at (Why you NEED AI):
- Processing thousands of data points quickly
- Spotting subtle patterns across large datasets
- Maintaining consistent attention to every detail

The Partnership Insight

Neither partner is "better" than the other. Each has genuine strengths AND genuine limitations. Real cybersecurity professionals succeed by knowing when to rely on which capabilities—including knowing their own limitations.

Suggested Opening Prompt (for structured data only): > "You're my cybersecurity investigation partner. We're analyzing account lockouts at a middle school. Here's the login log data and network observations: [share Documents A, B, D]. What patterns do you see in this structured data?"

Record AI Insights:

1. Patterns AI identified in structured data: _____
2. Additional questions AI raised: _____
3. What AI said it COULDN'T analyze: _____

Part 2B: Mutual Accountability Check

Critical Thinking Checkpoint: Good partnerships involve mutual accountability. Before acting on your combined findings:

CC BY 4.0

AI Finding	How would you verify this?	What other sources should you check?	What if AI is wrong?

Key Questions:

1. Did AI explain its reasoning, or just give an answer? _____
2. Could you confirm AI's pattern detection by looking at the data yourself? _____
3. What's the WORST that could happen if you act on AI's analysis without verifying? _____

Part 3: Team Synthesis

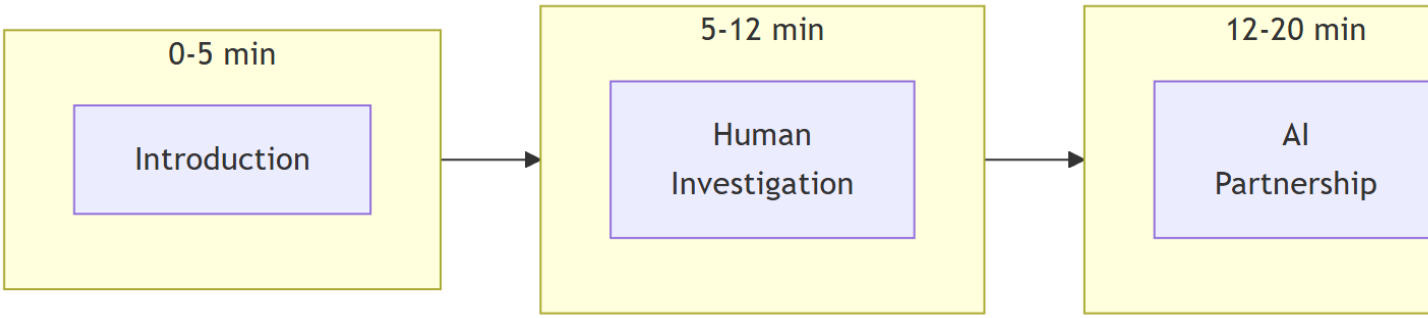
Combining Human + AI Strengths:

Investigation Aspect	Human Strength	AI Contribution	Combined Insight
Structured Data (Docs A, B, D)	Verify AI findings	Pattern detection	
Social Context (Doc C)	Understand intentions	*Cannot do this*	
Ethical Considerations	Judge right/wrong	Identify options	
Taking Action	Bear ethical responsibility	Inform the decision	

The Key Insight: Neither could have solved this alone. AI contributed _____, humans contributed _____, and TOGETHER we discovered _____.

Facilitation Guide

Activity Timeline (45 minutes)



Investigation Timeline

CC BY 4.0

Time	Phase	Instructor Actions	Student Activities
0-5 min	Introduction	Present scenario, distribute materials	Form teams, review evidence
5-12 min	Human Investigation	Circulate, prompt critical thinking	Complete Part 1 (focus on Document C - social context)
12-20 min	AI Partnership	Guide AI interactions, troubleshoot	Complete Part 2 (share Documents A, B, D with AI)
20-25 min	Verification	Emphasize "trust but verify"	Complete Part 2B verification checklist
25-35 min	Synthesis	Facilitate team discussions	Complete Part 3 synthesis worksheet
35-45 min	Debrief	Lead whole-class discussion	Share findings, reflect on partnership

Differentiation Strategies

For Advanced Students

- Add complexity: Introduce false leads in evidence
- Extend investigation: Multiple incident scenarios
- Leadership role: Facilitate other groups' investigations

For Struggling Students

- Provide evidence analysis templates
- Pre-highlight key patterns in documents
- Pair with stronger analytical partner
- Offer guided AI prompts list

For ELL Students

- Visual evidence representations
- Vocabulary support sheet
- Native language AI interactions (where available)
- Peer translation support

Common Challenges & Solutions

Troubleshooting Guide

Challenge: Students treat AI like Google - **Solution**: Model team member language, emphasize conversation vs. search
Challenge: AI provides incorrect analysis - **Solution**: Use as teaching moment about AI limitations, emphasize human verification
Challenge: Students skip the verification step - **Solution**: Require completed Part 2B before moving to synthesis; ask "How do you KNOW AI is right?"
Challenge: AI claims to analyze social context (Document C) - **Solution**: Point out that AI is guessing—it can't actually see social media posts or understand context

CC BY 4.0

Challenge: Limited device access - **Solution**: Rotate devices, use teacher demonstration, prepare printed AI responses
Challenge: Students over-rely on AI - **Solution**: Enforce "human first" investigation phase, require justification for AI consultation

Debrief Framework

Whole-Class Discussion Questions

1. **Discovery Questions**
   - What insights emerged that NEITHER human nor AI would have found alone?
   - What did humans contribute that AI couldn't? What did AI contribute that humans couldn't?
   - How did the partnership create something new—not just a combination of parts?
2. **Work Role Connections**
   - How would a real SOC Analyst partner with AI in their daily work?
   - What unique human capabilities matter in cybersecurity? What unique AI capabilities matter?
   - Which NICE Framework Work Roles interest you after this activity?
3. **Critical Thinking**
   - Who bears responsibility when a human-AI team makes a mistake?
   - How do we build trust in our AI partners while maintaining accountability?
   - What ethical considerations arise when humans and AI share decision-making?

Assessment Rubric

Criteria	Emerging (1)	Developing (2)	Proficient (3)	Advanced (4)
Collaboration Understanding	Views AI as tool only	Recognizes AI as assistant	Demonstrates true partnership	Articulates complementary strengths
Investigation Quality	Surface-level analysis	Identifies basic patterns	Systematic investigation	Comprehensive multi-layered analysis
NICE Framework Application	No connection to Work Roles	Basic role awareness	Clear role connections	Explores career pathways
Evidence Synthesis	Lists findings separately	Some integration attempted	Well-integrated conclusions	Novel insights from synthesis

Assessment Connection

This table shows how activity elements connect to assessment rubric criteria:

CC BY 4.0

Rubric Criterion	Developed Through	Evidence Source
AI Partnership Framing	Part 2: "Frame AI as team member, not search engine"	Worksheet: How student opened conversation with AI
Complementary Strengths	Part 2: "What AI Can and Can't Do" callout	Worksheet Part 2: Recording AI insights vs. limitations
AI Limitation Awareness	Part 2B: Mutual Accountability Check	Verification checklist completion
Synthesis Quality	Part 3: Team Synthesis table	"Key Insight" statement combining human + AI contributions
Decision Justification	Part 2B: "What if AI is wrong?"	Written response on accountability checklist
NICE Framework Application	Debrief: Work Role Connections	Verbal responses to career pathway questions

Applicable Rubrics: Human-AI Collaboration Rubric, Decision-Making Quality Rubric

Extension Activities

Take-Home Challenges

1. **Password Security Audit**: Students use AI to evaluate their own password practices (with parent permission)
2. **Social Engineering Awareness**: Create a presentation about social media safety using investigation insights
3. **Career Exploration**: Research one NICE Framework Work Role and interview a professional (virtually)

Cross-Curricular Connections

- **English/Language Arts**: Write a detective story featuring human-AI partnership
- **Mathematics**: Statistical analysis of breach patterns
- **Social Studies**: Research famous cybersecurity incidents and investigation methods
- **Science**: Explore pattern recognition in nature vs. algorithms

Implementation Resources

Required Materials Checklist

☐ Investigation evidence packets (printed or digital)
☐ Student worksheets (1 per student)
☐ Internet-enabled devices (minimum 1 per group)
☐ Projection system for demonstrations
☐ Timer for activity phases
☐ Optional: Role badges or cards for team assignments

AI Platform Quick Start Guides

ChatGPT Setup

CC BY 4.0

1. Navigate to chat.openai.com
2. Create free account or use shared credentials
3. Start new conversation for each group
4. Save conversation for assessment

Claude Setup

1. Navigate to claude.ai
2. Create free account or use shared credentials
3. Use "New Conversation" for each investigation
4. Export findings for documentation

Alternative: Local AI Options

- Use school-approved AI platforms
- Consider Bing Chat (Microsoft account)
- Google Bard with education accounts
- Pre-generated responses for offline environments

Instructor Reflection Guide

Post-Activity Reflection Questions

Student Engagement - Which evidence pieces generated the most discussion? - How did students' AI interaction skills evolve during the activity? - What misconceptions about AI emerged and how were they addressed?

Learning Outcomes - Did students achieve the collaboration understanding objective? - How effectively did students connect to NICE Framework Work Roles? - What evidence of career interest emerged?

Implementation Notes - What technical challenges arose and solutions found? - Which differentiation strategies proved most effective? - How could the activity be adapted for your specific context?

Future Iterations - Additional evidence types to include: _____ - AI platform preferences: _____ - Timing adjustments needed: _____

CC BY 4.0