AI-Assisted Incident Response

Quick-Start Guide for Educators

The Big Idea (Read This First)

This isn't "students learn about cyberattacks." It's **students experiencing how cybersecurity professionals actually work together during crises**—with AI as a critical team member.

The shift:

Old Framing	This Activity
Cybersecurity is individual heroics	Cybersecurity is coordinated teamwork
AI replaces human analysts	AI and humans have complementary strengths
Response means following procedures	Response requires judgment under pressure

What students should discover (don't tell them—let them find it):

- Different roles bring different essential perspectives
- AI excels at speed and pattern recognition; humans excel at context and judgment
- Real incidents require trade-offs with no perfect answers
- Time pressure changes how teams make decisions

The Scenario Framework

Teams respond to a realistic security incident, with each member taking a specific role. AI serves as the technical analyst partner, providing analysis that humans must interpret and act upon.

Core scenarios across grade bands:

- **K-2:** Computers won't turn on (robot helper finds the problem)
- **3-5:** Malware/pop-ups on classroom computers (investigation team)
- **6-8:** Ransomware, data breach, or social media compromise
- **9-12:** APT-level attack on enterprise with technical evidence

The Flow

Phase	Time	What's Happening	Your Role
1. Initial Assessment	10 min	Teams review evidence, assign roles, get AI analysis	Ensure all team members engage; help with role assignment
2. Response Planning	15 min	Teams analyze findings, develop response plan	Push for documented reasoning, not just decisions

Phase	Time	What's Happening	Your Role
3. Response Execution	15 min	Teams execute plan while handling complications	Inject complications at 5-min intervals
4. After-Action Review	10 min	Teams debrief, connect to careers	Focus on collaboration quality, not "right" answers

Critical Facilitation Moves

During Phase 1 (Initial Assessment):

> "Each role sees something different. Before you share with your team, make sure YOU understand what your role uniquely contributes."

This matters because students need to experience the value of specialization before collaboration.

During Phase 2 (Response Planning):

> "The AI gave you a recommendation. Before you follow it, ask: What does AI know? What doesn't it know?"

Watch for: Students accepting AI recommendations without critical evaluation. Redirect: "What context might AI be missing here?"

During Phase 3 (Response Execution):

> "Here's a complication…" [inject new development]

Watch for: Teams freezing or abandoning their plan entirely. Redirect: "How does this change your priorities? What stays the same?"

During Phase 4 (After-Action Review):

> "What could ONLY humans have contributed to this response? What could ONLY AI have contributed?"

This is the key learning moment—don't rush it.

Materials Needed

- ☐ Student worksheets (1 per student) — *see separate printables*
- ☐ Role cards (1 set per team) — *for role assignment*
- ☐ Incident briefing (1 per team) — *scenario description*
- ☐ Evidence packets (1 set per team) — *for 6-8 and 9-12 versions*
- ☐ AI response cards (for low-resource option)
- ☐ Complication cards (for Phase 3 injections)
- ☐ Timer
- ☐ Whiteboard for team status tracking

Low-resource option: Use AI Response Cards as printed handouts. The teacher reads AI analysis aloud or teams draw cards. The roleplay and collaboration still deliver the same learning.

Role Assignments

For Grades 6-8 and 9-12 (4-5 roles):

Role	Primary Responsibility	AI Partnership Focus
Incident Commander	Final decisions, coordination	Impact assessment, prioritization
SOC Analyst / Lead Analyst	Technical investigation	Pattern recognition, log analysis
Threat Intelligence	Attacker context, TTPs	Threat correlation, campaign mapping
Communications	Stakeholder messaging, documentation	Clear explanation generation
Evidence Coordinator (optional)	Chain of custody, forensics	Evidence organization

For Grades 3-5 (4 roles):

Role	Primary Responsibility
Detective	Looks at clues, notices patterns
AI Partner	Asks questions, shares AI responses
Recorder	Documents findings and decisions
Reporter	Presents team findings to class

For Grades K-2 (3-4 roles, whole class):

Role	What They Do
Detective	"What do you see?"
Thinker	"What might have caused this?"
Robot Helper	Teacher-voiced; "I can check things!"
Helper	"I'll try that!"

The Debrief Questions That Matter

1. "What did your role contribute that others couldn't?" *(Specialization value)*
2. "Where did AI help? Where did it fall short?" *(Partnership calibration)*
3. "What trade-offs did you make?" *(No perfect answers)*
4. "What was hardest about working under time pressure?" *(Real-world reality)*
5. "What NICE Framework careers do this work?" *(Career connection)*

If Things Go Wrong

Problem	It's Actually	Do This
One person dominates	Role boundaries unclear	"Each role needs to contribute. Detective, what did YOU notice?"
Team accepts AI blindly	Haven't found AI limitations yet	"What can't AI know about this situation? What context is it missing?"
Team ignores AI completely	Treating AI as optional	"You have an expert analyst available. Why not consult them?"
Team can't decide	Afraid of wrong answer	"In real incidents, delayed decisions have costs too. What's your best option now?"
Complications overwhelm team	Normal stress response	"Prioritize. What's the ONE thing you need to address first?"

Complication Injection Tips

Inject complications during Phase 3 to simulate real incident dynamics:

Timing: Every 5 minutes introduce one complication per team

Escalation: Start mild, increase pressure

Example sequence: 1. "Media has picked up the story—reporters are calling" 2. "New systems are showing signs of compromise" 3. "The CEO wants an update in 10 minutes" 4. "A parent group is organizing a meeting for tonight"

Purpose: Test adaptation without overwhelming. If a team is struggling, offer a simpler complication or pause.

Grade-Band Notes

Grade Band	Version Name	Key Adaptations
K-2	Fix It Team!	Whole class; teacher voices robot; focus on teamwork; 20-25 min
3-5	Computer Problem Solvers	4-person teams; malware investigation; structured steps; 35-40 min
6-8	AI-Assisted Incident Response	Full team roles; scenario options; complications; 50-60 min
9-12	SOC Analyst Simulation	Technical evidence; MITRE ATT&CK; executive communications; 55-60 min

From "True Teamwork: Building Human-AI Partnerships" — NICE K12 2025 Dr. Ryan Straight, University of Arizona • ryanstraight@arizona.edu

CC BY 4.0